

Inhaltsverzeichnis

1 Die G Data Business Software	3
1.1 G Data AntiVirus Business	3
1.2 G Data AntiVirus Enterprise	3
1.3 G Data ClientSecurity Business	3
1.4 G Data ClientSecurity Enterprise	3
1.5 G Data EndpointProtection Business	3
1.6 G Data EndpointProtection Enterprise	3
2 Allgemeines	10
2.1 PremiumHotline	10
2.2 Systemvoraussetzungen	10
2.3 Erste Schritte	10
2.4 G Data BootScan	10
3 Installation	15
3.1 G Data ManagementServer	15
3.2 G Data Administrator	15
3.3 G Data WebAdministrator	15
3.4 G Data Security Clients	15
3.5 G Data MailSecurity	15
4 G Data ManagementServer	22
5 G Data Administrator	23
5.1 Menüleiste	23
5.2 Clientauswahlbereich	23
5.3 Aufgabenbereiche	23
5.4 Mobile Clients	23
6 G Data Security Client	83
6.1 Tray-Icon	83
7 G Data WebAdministrator	86
7.1 Programmaufbau des G Data WebAdministrators	86
8 G Data MailSecurity MailGateway	87

9 G Data MailSecurity Administrator	88
9.1 Programmbereiche	88
9.2 Menüleiste	88
10 FAQ Installation	105
10.1 Ich habe die G Data Software ohne Registrierung installiert. Wie kann ich die Software registrieren?	105
10.2 Ich möchte die Installation der Clients zentral vom Server aus über den G Data Administrator durchführen	105
10.3 Ich möchte den G Data Administrator auf einem Client-Rechner installieren	105
10.4 Ich möchte die Clients mit Hilfe der G Data-CD-ROM mit der Client-Software ausstatten	105
10.5 Nach der Installation des Clients laufen einige Anwendungen erheblich langsamer als vorher	105
11 FAQ Allgemeines	108
11.1 MailSecurity, Exchange-Server 2000 und AVM Ken!	108
11.2 Wie kann ich überprüfen, ob die Clients eine Verbindung zum G Data ManagementServer haben?	108
11.3 Mein Postfach wurde in die Quarantäne geschoben	108
11.4 Der MMS soll nicht über seinen Namen, sondern über die IP-Adresse angesprochen werden	108
11.5 Speicherorte und Pfade	108
12 FAQ Linux-Nutzung	110
12.1 Linux-Fileserver Clients: Es wird keine Verbindung zum G Data ManagementServer aufgebaut / Signaturen werden nicht aktualisiert	110
12.2 Installation der Client-Software auf Linux-Rechnern	110
13 FAQ Fehlermeldungen	113
13.1 Einige Clients melden "Die Virendatenbank ist beschädigt.". Was ist zu tun?	113
13.2 Fehlermeldung "Sie benötigen mindestens Microsoft Exchange Server 2007 SP1"	113
13.3 Einige Clients melden "Programmdateien wurden verändert oder sind beschädigt". Was ist zu tun?	113

1 Die G Data Business Software

In Zeiten der weltweiten Vernetzung und den daraus resultierenden massiven Sicherheitsrisiken, ist das Thema Virenschutz nicht länger nur für IT-Fachleute von Interesse. Es muss vielmehr im Rahmen eines umfassenden, unternehmensweiten Risikomanagements auf höchster Managementebene betrachtet werden. Ein durch Viren verursachter Ausfall des Computernetzwerks trifft ein Unternehmen an seiner empfindlichsten Stelle. Die Folgen: Stillstand lebenswichtiger Systeme, Verlust erfolgsrelevanter Daten, Ausfall wichtiger Kommunikationskanäle. Computerviren können einem Unternehmen Schäden zufügen, von denen es sich nie mehr erholt!

G Data bietet Ihnen High-End Virenschutz für Ihr gesamtes Netzwerk. Die führende Sicherheitsleistung der G Data-Produkte wird seit Jahren in zahlreichen Tests mit Traumnoten prämiert. Die G Data Business-Software setzt konsequent auf zentrale Konfiguration und Verwaltung sowie größtmögliche Automatisierung. Alle Clients, ob Workstation, Notebook oder Fileserver, werden zentral gesteuert. Sämtliche Client-Prozesse laufen transparent im Hintergrund ab. Automatische Internet-Updates sorgen im Ernstfall einer Virenattacke für extrem kurze Reaktionszeiten.

Die zentrale Steuerung mit dem G Data ManagementServer ermöglicht Installation, Einstellungen, Updates, Fernsteuerung und Automatik für das gesamte Netzwerk. Das entlastet den Systemadministrator, spart Zeit und Kosten.

Wir wünschen Ihnen erfolgreiches und sicheres Arbeiten mit Ihrer G Data Business-Software.

Ihr G Data-Team

Versionsinformation

In dieser Dokumentation ist die Funktionalität aller G Data Business-Module beschrieben. Sollten Sie bei Ihrer installierten Software-Version ein Feature vermissen, können Sie über die **G Data Premium Hotline** bequem Informationen zum Upgrade Ihrer Software erhalten.

Produktübersicht	AntiVirus	Firewall	AntiSpam	Policy Manager	MailSecurity	Backup
G Data AntiVirus Business	★					
G Data AntiVirus Enterprise	★				★	★
G Data MailSecurity					★	
G Data ClientSecurity Business	★	★	★			
G Data ClientSecurity Enterprise	★	★	★		★	★
G Data EndpointProtection Business	★	★	★	★		
G Data EndpointProtection Enterprise	★	★	★	★	★	★

Copyright-Information

Copyright © 2012 G Data Software AG

Engine A: The Virus Scan Engine and the Spyware Scan Engines are based on BitDefender technologies © 1997-2012 BitDefender SRL.

Engine B: © 2012 Alwil Software

OutbreakShield: © 2012 Commtouch Software Ltd.

[G Data - 06.11.2012, 13:20]

1.1 G Data AntiVirus Business

Schützt Ihre Unternehmensdaten mit leistungsstarken Sicherheitstechnologien über einen zentral gesteuerten Virenschutz. Der in der Version 12 komplett überarbeitete Administrator besticht durch übersichtlichen Aufbau und einfachste Bedienung. Sämtliche Clients auf Workstations, Notebooks und Fileservern werden über den ManagementServer gesteuert. Dabei laufen alle Client-Prozesse unsichtbar im Hintergrund ab und Anwender können ihnen zugewiesene Sicherheitslevel nicht ändern. Das Add-In für Outlook 2010 erkennt zuverlässig Viren-Mails. Bei PC-Inaktivität startet der Leerlaufscan selbstständig die Überprüfung.

Testsieger-Sicherheitspaket

- DoubleScan-Technologie für beste Virenerkennung
- Selbstlernendes Fingerprinting und Whitelisting bei ungebremsster PC-Leistung
- Modernste Methoden zur Erkennung unbekannter Viren (Behaviour Blocking, Heuristik, Cloud Security)

G Data ManagementServer und G Data Administrator

- ActiveDirectory-Anbindung zur Übernahme bestehender Gruppenstrukturen und automatischer Client-Installation.
- Einbindung von PCs aus Fremddomänen
- Dashboard für alle relevanten Informationen (Reportstatus, Top-Ten infizierte Clients uvm.)
- Installation, Virensuche, Updates, Einstellungen und Reports ferngesteuert im Netz (LAN/WAN)
- Wiederherstellung älterer Signaturstände (Rollback) bei unerwarteten Problemen
- NEU! Zentrales Management von firmengenutzten Android-Endgeräten mit Rückmeldung eventueller Virenfunde und des Sicherheitsstatus
- NEU! Soft- und Hardwareverzeichnis für die Clients – leichte Verwaltung der Clients durch eine detaillierte Darstellung des Inventars
- NEU! Ausführliche Analysen und Berichte zur Malwaresituation im Netzwerk
- Optionales Silverlight Web-Interface
- NEU! Optionales Mobile-Browser-Interface
- Kaskadierung und Ausfallschutz der Serversoftware
- Wiederherstellung älterer Signaturstände (Rollback)
- Erstellung von Client-Installationspaketen

G Data Security Client

- Client-Schutz für User „unsichtbar“ im Hintergrund
- NEU! BankGuard Schutz für sicherer Online Zahlungsverkehr
- Add-In für Outlook 2010 zur Erkennung von Viren
- E-Mail-Virenblocker für POP3 und IMAP
- Volle Funktion im Offsite-Betrieb
- Anti-Virus Linux-Clients

1.2 G Data AntiVirus Enterprise

Der High-End-Virenschutz für Firmennetzwerke. Mit zentraler Steuerung und automatischem Schutz für alle Mail- und Fileserver, Workstations und Notebooks. Der komplett überarbeitete Administrator garantiert einfachste Bedienung und beste Übersicht.

Alle G Data Enterpriseversionen besitzen zudem ein neues Backup-Modul zur Datensicherung sowie G Data MailSecurity, den leistungsstarken Virenschutz für die gesamte Mail-Korrespondenz Ihres Unternehmens. G Data MailSecurity ist als Virenschutz-Plug-in für Microsoft Exchange Server oder als Mailserver-unabhängiges Mail-Gateway einsetzbar.

Testsieger-Sicherheitspaket

- DoubleScan-Technologie für beste Viren-erkennung
- Selbstlernendes Fingerprinting und Whitelisting bei ungebremsster PC-Leistung

- Modernste Methoden zur Erkennung unbekannter Viren (Behaviour Blocking, Heuristik, Cloud Security)

G Data Security Client

- Client-Schutz für User „unsichtbar“ im Hintergrund
- NEU! BankGuard Schutz für sicherer Online Zahlungsverkehr
- Add-In für Outlook 2010 zur Erkennung von Viren
- E-Mail-Virenblocker für POP3 und IMAP
- Volle Funktion im Offsite-Betrieb
- Voll integrierte Anti-Virus Linux-Clients

G Data ManagementServer

- ActiveDirectory-Anbindung zur Übernahme bestehender Gruppenstrukturen und automatischer Client-Installation.
- Einbindung von PCs aus Fremddomänen
- Dashboard für alle relevanten Informationen (Reportstatus, Top-Ten infizierte Clients uvm.)
- Installation, Virensuche, Updates, Einstellungen und Reports ferngesteuert im Netz (LAN/WAN)
- Optionales Silverlight Web-Interface
- Kaskadierung und Ausfallschutz der Serversoftware
- Wiederherstellung älterer Signaturstände (Rollback)
- NEU! Optionales Mobile-Browser-Interface

G Data MailSecurity

- Viren- und Spamfilter als Mailserver-unabhängige Gateway-Lösung (SMTP / POP3)
- Für beliebige Mailserver wie Exchange, Notes etc.
- MailSecurity AntiVirus Plug-in für MS-Exchange

G Data Backup

- Transparentes File-Backup ins Firmennetzwerk
- Voll-Backup und differentielles Backup

1.3 G Data ClientSecurity Business

Das ideale Werkzeug für moderne, leistungsfähige Unternehmensnetzwerke. Ganz gleich, ob mobil oder stationär, sämtliche Clients sind zentral steuerbar und erhalten höchstmöglichen Schutz, ohne ihre Leistungsfähigkeit einzubüßen. Schnell und effizient sichert der client/server-basierte Testsieger-Virenschutz das gesamte Netzwerk und garantiert dabei einfachste Bedienung und beste Übersicht.

Testsieger-Sicherheitspaket

- DoubleScan-Technologie für beste Virenerkennung
- Selbstlernendes Fingerprinting und Whitelisting bei ungebremster PC-Leistung
- Modernste Methoden zur Erkennung unbekannter Viren (Behaviour Blocking, Heuristik, Cloud Security)

G Data Security Client

- Client-Schutz für User „unsichtbar“ im Hintergrund
- NEU! Add-In für Outlook 2010 zur Erkennung von Viren- und Spam-Mails
- E-Mail-Virenblocker für POP3 und IMAP
- Volle Funktion im Offsite-Betrieb
- Voll integrierte Linux-Clients

G Data ManagementServer und G Data Administrator

- NEU! ActiveDirectory-Anbindung zur Übernahme bestehender Gruppenstrukturen und automatischer Client-Installation.
- NEU! Einbindung von PCs aus Fremddomänen

- NEU! Dashboard für alle relevanten Informationen (Reportstatus, Top-Ten infizierte Clients uvm.)
- Installation, Virensuche, Updates, Einstellungen und Reports ferngesteuert im Netz (LAN/WAN)
- NEU! Optionales Silverlight Web-Interface
- Kaskadierung und Ausfallschutz der Serversoftware
- Wiederherstellung älterer Signaturstände (Rollback)
- Neu! Optionales Mobile-Browser-Interface

G Data Firewall Client

- NEU! Vereinfachte Firewall-Ansicht
- 100 % zentrale Administration
- Autopilot oder zentrale Regelsätze
- Einfaches Erstellen von Regeln per Dialog, Assistent oder aus Berichten
- Auflistung geblockter Anwendungen
- Optionale Offsite-Konfiguration für Notebooks

G Data AntiSpam Client

- Clientseitiges Spam-OutbreakShield
- Vielfach ausgezeichnete Spam-Echtzeitschutz

1.4 G Data ClientSecurity Enterprise

Ihr High-End-Rundumschutz mit 100 % zentral gesteuerter Administration für mobile und stationäre Clients plus effektivem Spam- und Phishingschutz. Die neue Generation des Testsieger-Virenschutzes arbeitet ohne Performance-Einschränkungen und mit komplett überarbeitetem Administrator, der einfachste Bedienung und beste Übersicht garantiert.

Alle G Data Enterpriseversionen besitzen zudem ein neues Backup-Modul zur Datensicherung sowie G Data MailSecurity, den leistungsstarken Viren- und Spamschutz für die gesamte Mail-Korrespondenz Ihres Unternehmens. G Data MailSecurity ist als Virenschutz-Plug-in für Microsoft Exchange Server oder als Mailserver-unabhängiges Mail-Gateway einsetzbar.

Testsieger-Sicherheitspaket

- DoubleScan-Technologie für beste Virenerkennung
- Selbstlernendes Fingerprinting und Whitelisting bei ungebremster PC-Leistung
- Modernste Methoden zur Erkennung unbekannter Viren (Behaviour Blocking, Heuristik, Cloud Security)

G Data Security Client

- Client-Schutz für User „unsichtbar“ im Hintergrund
- NEU! Add-In für Outlook 2010 zur Erkennung von Viren- und Spam-Mails
- E-Mail-Virenblocker für POP3 und IMAP

G Data AntiSpam Client

- Clientseitiges Spam-OutbreakShield
- Vielfach ausgezeichnete Spam-Echtzeitschutz

G Data ManagementServer und G Data Administrator

- NEU! ActiveDirectory-Anbindung zur Übernahme bestehender Gruppenstrukturen und automatischer Client-Installation.
- NEU! Einbindung von PCs aus Fremddomänen
- NEU! Dashboard für alle relevanten Informationen (Reportstatus, Top-Ten infizierte Clients uvm.)
- Installation, Virensuche, Updates, Einstellungen und Reports ferngesteuert im Netz (LAN/WAN)
- NEU! Optionales Silverlight Web-Interface

G Data Firewall Client

- NEU! Vereinfachte Firewall-Ansicht

- 100 % zentrale Administration
- Autopilot oder zentrale Regelsätze
- Einfaches Erstellen von Regeln
- Optionale Offsite-Konfiguration für Notebooks

G Data MailSecurity

- Viren- und Spamfilter als Mailserver-unabhängige Gateway-Lösung (SMTP / POP3)
- Für beliebige Mailserver wie Exchange, Notes etc.
- NEU! MailSecurity AntiVirus Plug-in für MS-Exchange

G Data Backup

- Transparentes File-Backup ins Firmennetzwerk
- Voll-Backup und differentielles Backup

1.5 G Data EndpointProtection Business

Die zu 100 % zentral gesteuerte All-In-One Sicherheitslösung für kleine, mittlere und große Unternehmensnetzwerke erscheint in der zweiten Generation. Mit weiter verbessertem Schutz vor Malware-Bedrohungen für Notebooks, Workstations und Server, dem PolicyManager für individuelle Geräte-, Applikations- und Internetkontrolle sowie Content Filter zur Sicherstellung Ihrer Firmen-Policy am Arbeitsplatz.

Zusammen mit Client-Firewall, Leerlauf-Scan und effizienten, produktivitäts-steigernden Client-Einstellungen sorgt auch die neue Version des G Data Flaggschiffs für höchste Sicherheit vor Hackerattacken, Viren und Spam sowie Rechtssicherheit im Umgang mit Unternehmens-PCs.

Testsieger-Sicherheitspaket

- DoubleScan-Technologie für beste Virenerkennung
- Selbstlernendes Fingerprinting und Whitelisting bei ungebremster PC-Leistung
- Modernste Methoden zur Erkennung unbekannter Viren (Behaviour Blocking, Heuristik, Cloud Security)

G Data Security Client

- Client-Schutz für User „unsichtbar“ im Hintergrund
- NEU! Add-In für Outlook 2010 zur Erkennung von Viren- und Spam-Mails
- E-Mail-Virenblocker für POP3 und IMAP
- Volle Funktion im Offsite-Betrieb
- Voll integrierte Linux-Clients

G Data AntiSpam Client

- Clientseitiges Spam-OutbreakShield
- Vielfach ausgezeichneter Spam-Echtzeitschutz

G Data ManagementServer und G Data Administrator

- NEU! ActiveDirectory-Anbindung zur Übernahme bestehender Gruppenstrukturen und automatischer Client-Installation.
- NEU! Einbindung von PCs aus Fremddomänen
- NEU! Dashboard für alle relevanten Informationen
- Installation, Virensuche, Updates, Einstellungen und Reports ferngesteuert im Netz (LAN/WAN)
- NEU! Optionales Silverlight Web-Interface

G Data Firewall Client

- NEU! Vereinfachte Firewall-Ansicht
- 100 % zentrale Administration
- Einfaches Erstellen von Regeln per Dialog, Assistent oder aus Berichten
- Auflistung geblockter Anwendungen

- Optionale Offsite-Konfiguration für Notebooks

G Data PolicyManager

- NEU! Mailbenachrichtigung des PolicyManagers
- Geräte-Kontrolle: USB- und Firewire-Massenspeichergeräte; Webcams; CD/DVD Medienkontrolle
- Anwendungskontrolle: Black- und Whitelisting / Vordefinierbare Anwendungen (Games etc.)
- Content Filter mit über 80 vordefinierten Kategorien, z. B. Sex/Pornografie/Gewalt; Chats/Foren/Blogs
- Internetnutzungskontrolle: Stundengenaue Sperrzeiten (Tag); limitierte Nutzungszeiten (Tag, Woche und Monat)

1.6 G Data EndpointProtection Enterprise

Mit weiter verbessertem Schutz vor Malware-Bedrohungen für Notebooks, Workstations und Server, dem PolicyManager für individuelle Geräte-, Applikations- und Internetkontrolle sowie Content Filter zur Sicherstellung Ihrer Firmen-Policy am Arbeitsplatz. Der client/server-basierte Testsieger-Virenschutz sichert Ihr gesamtes Unternehmensnetzwerk und überzeugt durch einfachste Bedienung und Übersichtlichkeit. Client-Firewall, Leerlauf-Scan und produktivitätsunterstützende Client-Einstellungen gehören ebenso zum Leistungsumfang wie das neue Backup-Modul für bestmögliche Datensicherung.

Testsieger-Sicherheitspaket

- DoubleScan-Technologie für beste Virenerkennung
- Selbstlernendes Fingerprinting und Whitelisting bei ungebremsster PC-Leistung
- Modernste Methoden zur Erkennung unbekannter Viren (Behaviour Blocking, Heuristik, Cloud Security)

G Data ManagementServer und G Data Administrator

- NEU! ActiveDirectory-Anbindung zur Übernahme bestehender Gruppenstrukturen und automatischer Client-Installation.
- NEU! Einbindung von PCs aus Fremddomänen
- NEU! Dashboard für alle relevanten Informationen
- Installation, Virensuche, Updates, Einstellungen und Reports ferngesteuert im Netz (LAN/WAN)
- NEU! Optionales Silverlight Web-Interface
- Kaskadierung und Ausfallschutz der Serversoftware
- Wiederherstellung älterer Signaturstände (Rollback)

G Data Security Client

- Client-Schutz „unsichtbar“ im Hintergrund
- NEU! Add-In für Outlook 2010 zur Erkennung von Viren- und Spam-Mails
- E-Mail-Virenblocker für POP3 und IMAP
- Volle Funktion im Offsite-Betrieb

G Data AntiSpam Client

- Clientseitiges Spam-OutbreakShield
- Vielfach ausgezeichnete Spam-Echtzeitschutz

G Data Firewall Client

- NEU! Vereinfachte Firewall-Ansicht
- 100 % zentrale Administration
- Einfaches Erstellen von Regeln per Dialog, Assistent oder aus Berichten
- Auflistung geblockter Anwendungen

G Data MailSecurity

- Viren- und Spamfilter als Mailserver-unabhängige Gateway-Lösung (SMTP / POP3)
- NEU! MailSecurity AntiVirus Plug-in für MS-Exchange

G Data PolicyManager

- NEU! Mailbenachrichtigung des PolicyManagers
- Geräte-Kontrolle: USB- und Firewire-Massenspeichergeräte; Webcams; CD/DVD Medienkontrolle
- Anwendungskontrolle: Black- und Whitelisting / Vordefinierbare Anwendungen (Games etc.)
- Content Filter mit über 80 vordefinierten Kategorien, z. B. Sex/Pornografie/Gewalt; Chats/Foren/Blogs
- Internetnutzungskontrolle: Stundengenaue Sperrzeiten, limitierte Nutzungszeiten

G Data Backup

- Transparentes File-Backup ins Firmennetzwerk
- Voll-Backup und differentielles Backup

2 Allgemeines

2.1 PremiumHotline

Die **PremiumHotline** für G Data Netzwerklicenzen steht allen registrierten Business-Kunden jederzeit zur Verfügung.

Telefon: +49 234 9762 901

Nutzen Sie eine Flatrate, so ist das Supportgespräch nach den Tarifbedingungen ohne zusätzliche Kosten.

E-Mail: business-support@gdata.de

Viele Fragen und Sachverhalte sind auch schon im Supportbereich der G Data Website beantwortet worden. Besuchen Sie uns unter:

www.gdata.de

Die **Registriernummer** finden Sie je nach Art des Produktes auf der Lizenzurkunde (MediaPack) oder in der Auftragsbestätigung.

Kontaktieren Sie im Zweifelsfall Ihren Händler bzw. den betreuenden Distributor.

Überprüfen Sie vor Gesprächen mit der **Hotline**, wie Ihr Computer/Netzwerk ausgestattet ist. Wichtig sind dabei vor allem folgende Informationen:

- Die **Versionsnummern** des G Data Administrators und des G Data ManagementServers (diese finden Sie im **Hilfe**-Menü des G Data Administrators)
- Die **Registrierungsnummer** oder der **Benutzernamen** für das **Internet-Update**.
- Die genaue Windows-Version (Client/Server)
- Zusätzlich installierte Hard- und Softwarekomponenten (Client/Server)
- Eventuell auftretende Fehlermeldungen (inkl. Fehlercodes, sofern vorhanden) im genauen Wortlaut

Mit diesen Angaben wird das Gespräch mit den Support-Mitarbeitern kürzer, effektiver und erfolgreicher verlaufen. Wenn möglich, platzieren Sie das Telefon in der Nähe eines Rechners, auf dem der G Data Administrator installiert ist.

Internet-Ambulanz

Sollten Sie einen neuen Virus oder ein unbekanntes Phänomen feststellen, senden Sie uns in jedem Fall diese Datei über die Quarantäne-Funktion der G Data Software. Klicken Sie dazu im Bereich **Berichte** mit der rechten Maustaste auf einen Virusfund und wählen dort die Option **Quarantäne: Zur Internet-Ambulanz senden**. Wir analysieren den Virus und werden Ihnen möglichst schnell ein Gegenmittel zur Verfügung stellen. Selbstverständlich behandeln wir Ihre eingesandten Daten höchst vertraulich und diskret.

Die Rücksende-Adresse für Antworten von der Internet-Ambulanz können Sie im Bereich **Optionen > Server-Einstellungen > E-Mail-Einstellungen** definieren.

2.2 Systemvoraussetzungen

Folgende Mindestanforderungen werden an die Clients- bzw. Server gestellt:

- Windows 7 (32/64bit),
- Windows 8 (32/64bit)
- Windows Vista (32/64bit)
- Microsoft Windows XP (SP2 oder höher, 32bit) oder
- Windows Server 2003, 2008 und 2012

mit mindestens 1GB verfügbarem Arbeitsspeicher. Das G Data-System nutzt das **TCP/IP-Protokoll** zur Kommunikation von Client- und Server-Rechnern untereinander. Folgende Mindestanforderungen werden an die Clients- bzw. Server gestellt:

G Data Security Client

- Microsoft Windows Server 2008 (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Server 2008 R2 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Server 2012 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Small Business Server 2011 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Essential Business Server 2008 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Small Business Server 2008 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Essential Business Server 2012 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Server 2003 (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Small Business Server 2003 (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows 8 (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows 7 (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Vista (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows XP (SP2 oder höher, 32bit), 512 MB verfügbarer Arbeitsspeicher
- Linux, SMB ab 2.6.17: Ubuntu 6.10-9.04, Debian Etch/Lenny, SuSE/SLES 10/11, RHEL 5.3/Fedora 7-10, 512 MB verfügbarer Arbeitsspeicher
- Linux, WS ab 2.6.25: Ubuntu 8.10-9.10, Debian Lenny, SuSE/SLES 11, Fedora 9-12, 512 MB verfügbarer Arbeitsspeicher

Für **Linux-Rechner**, die als Fileserver arbeiten und verschiedenen Clients Windows-Freigaben (über das **SMB-Protokoll**) zur Verfügung stellen, kann manuell ein Modul installiert werden, das den Zugriff auf die Freigaben kontrolliert und bei jedem Zugriff einen Scan auf die Datei ausführt, so dass keine Malware vom **Samba-Server** auf die Windows-Clients (und umgekehrt) gelangen kann.

G Data ManagementServer

- Microsoft Windows Server 2008 (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Server 2008 R2 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Server 2012 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Small Business Server 2011 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Essential Business Server 2008 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Small Business Server 2008 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Essential Business Server 2012 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Server 2003 (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Small Business Server 2003 (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows 8 (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows 7 (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Vista (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows XP (SP2 oder höher, 32bit), 1 GB verfügbarer Arbeitsspeicher

G Data MailSecurity

- Microsoft Windows Server 2008 (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Server 2008 R2 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Server 2012 (64bit), 1 GB verfügbarer Arbeitsspeicher

- Microsoft Windows Small Business Server 2011 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Essential Business Server 2008 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Small Business Server 2008 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Essential Business Server 2012 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Server 2003 (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Small Business Server 2003 (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows 8 (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows 7 (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Vista (32/64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows XP (SP2 oder höher, 32bit), 1 GB verfügbarer Arbeitsspeicher

G Data MailSecurity (Plugin für Microsoft Exchange 2010)

- Microsoft Windows Server 2008 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Server 2008 R2 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Server 2012 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Small Business Server 2011 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Essential Business Server 2008 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Small Business Server 2008 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Essential Business Server 2012 (64bit), 1 GB verfügbarer Arbeitsspeicher

G Data MailSecurity (Plugin für Microsoft Exchange 2007 x64)

- Microsoft Windows Server 2008 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Server 2008 R2 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Server 2012 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Small Business Server 2011 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Essential Business Server 2008 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Small Business Server 2008 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Essential Business Server 2012 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Server 2003 (64bit), 1 GB verfügbarer Arbeitsspeicher
- Microsoft Windows Small Business Server 2003 (64bit), 1 GB verfügbarer Arbeitsspeicher

2.3 Erste Schritte

Führen Sie bei akutem Virenverdacht auf den betroffenen Rechnern erst einen **G Data BootScan** durch.

- Installieren Sie dann den **G Data ManagementServer** auf Ihrem Server. Bei der Installation des G Data ManagementServers wird automatisch der **G Data Administrator** auf dem Server installiert. Mit diesem Programm kann der G Data ManagementServer gesteuert werden. Um den optimalen Schutz zu gewährleisten, sollte der Rechner immer erreichbar (eingeschaltet) sein und für das automatische Laden der Virensignaturen über einen Internetzugang verfügen. Eine Installation des G Data ManagementServers muss nicht auf einem Serverbetriebssystem erfolgen (siehe **Systemvoraussetzungen**).
- Führen Sie nun die **Online-Registrierung** durch. Ohne eine Online-Registrierung können keine Aktualisierungen der Software erfolgen.
- Beim ersten Start des G Data Administrators auf dem Server startet der **Einrichtungsassistent**. Mit diesem kann die **Client-Software** auf den gewünschten Clients in Ihrem Netzwerk direkt installiert werden. Alle Einstellungen, die mit dem Einrichtungsassistenten vorgenommen werden, lassen sich auch nachträglich ändern.

- Sollten sich Probleme bei der **Remote-Installation** der Clients ergeben, kann die Client-Software natürlich auch mit Hilfe der G Data CD/DVD oder einem selbst erstellten Client-Installationspaket auf den Clients installiert werden. Damit auch der Server selbst vor Virenbefall geschützt ist, empfiehlt sich auch für den Server die Installation der Client-Software.

Client-Installationspakete können auch über GPO/Anmelde-Skripte verteilt werden.

- Nach erfolgter Einrichtung und Installation der Client-Software auf den angeschlossenen Maschinen kann der Virenschutz sowie die Internet-Updates der G Data Client- und Serversoftware zentral gesteuert werden.
Der G Data Administrator bietet unter anderem Einstellungsmöglichkeiten für den Echtzeitschutz durch den **G Data Wächter** sowie die Möglichkeit, Scanaufträge zu definieren, die das Netzwerk regelmäßig auf Virenbefall untersuchen.

Sollte es notwendig werden, ein Einstellungsproblem an einem Client vor Ort zu lösen, kann der G Data Administrator auf jedem Client innerhalb des Netzwerks installiert werden. Damit entfällt die Notwendigkeit, alle Einstellungen lokal am Server vorzunehmen.

Sollte es notwendig werden eine kritische Situation innerhalb Ihre Netzwerk außerhalb Ihre Unternehmen zu lösen, kann der G Data Web Administrator über jeden Desktop-Web-Browser verwendet werden. Mit dem G Data Mobile Administrator können Sie die Administration so unterwegs von Ihren Mobile-Web-Browser aus durchführen.

2.4 G Data BootScan

Der **G Data BootScan** erlaubt eine Bekämpfung von Viren, die sich vor der Installation der Antivirensoftware auf dem Rechner eingenistet haben und möglicherweise die Installation der G Data Software unterbinden möchten. Dazu gibt es eine spezielle Programmversion der G Data Software, die schon vor dem Systemstart ausgeführt werden kann.

Was mache ich, wenn mein Computer nicht von CD/DVD bootet? Sollte das System nicht von CD/DVD-ROM booten, kann es sein, dass diese Option erst eingestellt werden muss. Dies erfolgt im **BIOS**, einem System, das noch vor Ihrem Betriebssystem gestartet wird. Um hier Änderungen vorzunehmen, führen Sie folgende Schritte durch:

1. Schalten Sie den Computer aus.
2. Starten Sie Ihren Computer wieder. Üblicherweise gelangen Sie zum BIOS-Setup, indem Sie beim Hochfahren (= Booten) des Rechners die **Entf**-Taste (manchmal auch die Taste **F2**- oder **F10**-Taste) drücken. Die Dokumentation des Rechnerherstellers liefert hierzu weitere Hinweise.
3. Wie Sie die Einstellungen in Ihrem BIOS-Setup im Einzelnen ändern, entnehmen Sie der Dokumentation Ihres Mainboard-Herstellers. Im Ergebnis sollte die Bootreihenfolge **CD/DVD-ROM**, **C:** lauten, d.h. das CD/DVD-ROM-Laufwerk wird zum **1st Boot-Device** und die Festplatten-Partition mit Ihrem Windows-Betriebssystem zum **2nd Boot-Device**.
4. Speichern Sie die Änderungen und starten Sie Ihren Computer neu. Jetzt ist Ihr Computer bereit für einen BootScan.

Beim **G Data BootScan** gehen Sie folgendermaßen vor:

- 1a G Data BootScan mit der Programm-CD:** Legen Sie die **G Data Software DVD** in das Laufwerk. Klicken Sie auf dem sich öffnenden Startfenster auf **Abbrechen** und schalten Sie den Computer aus.
- 1b G Data BootScan mit selbst erstellter G Data BootCD:** Hierzu muss zunächst das Erstellungsprogramm für die G Data BootCD installiert werden. Dies muss auf einem System erfolgen, auf dem ein G Data Security Client mit aktuellen Signaturen installiert ist; befolgen sie die Anweisungen des G Data BootCD Wizards.

Nach dem ersten Schritt verläuft der BootScan für alle drei Varianten identisch:

- 2** Starten Sie den Computer neu. Es erscheint das Startmenü des **G Data BootScans**.

- 3** Wählen Sie mit den Pfeiltasten die Option **G Data BootCD** und bestätigen die Auswahl mit **Enter**. Es wird nun ein Linux-Betriebssystem von der CD/DVD gestartet und es erscheint eine G Data Spezialversion für BootScans.

Falls Sie Probleme mit der Ansicht der Programmoberfläche haben, starten Sie den Rechner erneut und wählen bitte die Option **G Data BootCD – Alternativ** aus.
- 4** Das Programm schlägt nun vor, die Virensignaturen zu aktualisieren. Klicken Sie hier auf **Ja** und führen Sie das Update durch. Sobald die Daten über das Internet aktualisiert wurden, erscheint die Meldung **Update erledigt**. Verlassen Sie nun den Update-Bildschirm mit Anklicken der **Schließen**-Schaltfläche.

Das automatische **Internet-Update** steht Ihnen dann zur Verfügung, wenn Sie einen **Router** verwenden, der IP-Adressen automatisch vergibt (**DHCP**). Sollte das Internet-Update nicht möglich sein, können Sie den **G Data BootScan** auch mit alten Virensignaturen durchführen. Dann sollten Sie allerdings nach der Installation der G Data Software möglichst bald einen neuen BootScan mit aktualisierten Daten durchführen. Wenn Sie eine G Data BootCD selbst erstellt haben, sind die Virensignaturen auf dem Updatestand, den der G Data Security Client zum Zeitpunkt der Erstellung der BootCD geladen hat.
- 5** Nun sehen Sie die Programmoberfläche. Klicken Sie auf den Eintrag **Überprüfe Computer** und Ihr Computer wird auf Viren und Schadsoftware untersucht. Dieser Vorgang kann je nach Rechnerart und Festplattengröße eine Stunde oder länger dauern.
- 6** Sollte die G Data Software Viren finden, entfernen Sie diese mit Hilfe der im Programm vorgeschlagenen Option. Nach einer *erfolgreichen* Entfernung des Virus steht Ihnen die Originaldatei weiter zur Verfügung.
- 7** Nach Abschluss der Virenüberprüfung klicken Sie auf die **Beenden**-Schaltfläche und wählen anschließend **Neu Starten** aus.

Die **Beenden**-Schaltfläche befindet sich unten rechts in der Linux-Programmoberfläche.
- 8** Entfernen Sie die **G Data BootCD** aus dem Laufwerk.
- 9** Schalten Sie ihren Computer wieder aus und starten Sie ihn erneut. Nun startet Ihr Computer wieder mit Ihrem Standard-Betriebssystem. Die G Data Software kann nun auf einem virenfreien System installiert werden.

3 Installation

Starten Sie Windows und legen die G Data DVD in Ihr DVD-Laufwerk ein. Es öffnet sich automatisch ein Installationsfenster. Schließen Sie alle anderen Programme, bevor Sie mit der Installation der G Data Software beginnen. Es kann zu Fehlfunktionen oder einem Abbruch kommen, falls z.B. Programme geöffnet sind, die auf Daten zugreifen, die die G Data Software zur Installation benötigt. Nachdem Sie die Schaltfläche **Installieren** gedrückt haben, erscheint ein Bildschirm, in dem Sie auswählen können, welche der G Data Software-Komponenten Sie installieren wollen. Folgende Installationsmöglichkeiten stehen zur Verfügung:

- **G Data ManagementServer:** Als erstes sollte der **G Data ManagementServer** auf dem Computer installiert werden, der alle G Data - relevanten Einstellungen und Updates verwalten soll. Der G Data ManagementServer ist das Herzstück der G Data Architektur: Er verwaltet die Clients, fordert neueste Software- und Virensignaturupdates automatisch vom G Data UpdateServer an und steuert den Virenschutz im Netzwerk. Mit der Installation des G Data ManagementServers wird automatisch die **G Data Administrator-Software** installiert, mit der der G Data ManagementServer gesteuert wird.
- **G Data Administrator:** Der **G Data Administrator** ist die Steuerungssoftware für den G Data ManagementServer, die die Verwaltung von Einstellungen und Updates für alle im Netzwerk installierten G Data - Clients ermöglicht. Der G Data Administrator ist passwortgeschützt und kann auf jedem Windows-Rechner innerhalb des Netzwerkes installiert und gestartet werden.
- **G Data Security Client:** Die **Client-Software** stellt den Virenschutz für die Clients bereit und führt die ihm vom G Data ManagementServer zugewiesenen Jobs ohne eigene Bedienoberfläche im Hintergrund aus. Die Installation der Client-Software erfolgt in der Regel zentral für alle Clients über den G Data Administrator.
- **G Data InternetSecurity:** Wenn Sie die SmallBusiness-Versionen der G Data Software nutzen, steht Ihnen die G Data InternetSecurity als zusätzlicher autonomer Schutz für Rechner zur Verfügung, die nicht mit Ihrem Netzwerk verbunden sind, z.B. Notebooks von Außendienstmitarbeitern.
- **G Data MailSecurity:** Wenn Sie eine Enterprise-Version der G Data Software verwenden, steht Ihnen auch das G Data MailGateway zur Installation zur Verfügung.
- **G Data BootCD-Erstellung:** Mit Hilfe des G Data BootCD Wizards können Sie eine bootfähige CD zur grundlegenden Überprüfung Ihres Rechners erstellen. Diese Überprüfung findet noch vor dem Start des installierten Betriebssystems statt. Dazu werden die aktuellen Virensignaturen verwendet. Mit einer erstellten G Data BootCD können Sie einen **BootScan** auch ohne die Original G Data-Software-DVD durchführen. Lesen Sie hierzu auch das Kapitel **G Data BootScan**.
- **G Data WebAdministrator:** Der **G Data WebAdministrator** ist eine webbasierte Steuerungssoftware für den G Data ManagementServer. Mit ihm können Einstellungen für den G Data ManagementServer über ein Webinterface in einem Browser vorgenommen werden. Er kann auf diese Weise ein Ersatz für die Installation des G Data Administrators sein.
- **G Data MobileAdministrator:** Der MobileAdministrator ist eine Web-basierende Steuerungssoftware für den ManagementServer. Er kann mit Hilfe eines Mobile-Web-Browsers gestartet werden und bietet Ihnen dieselben Funktionen wie der **G Data Administrator** und der **G Data WebAdministrator**.

Der MobileAdministrator steht Ihnen bei den Programmversionen AntiVirus, ClientSecurity und EndpointProtection (Business/Enterprise) zur Verfügung.

3.1 G Data ManagementServer



Legen Sie die G Data-DVD ein und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend die Komponente **G Data ManagementServer** durch einen Klick auf die nebenstehende Schaltfläche.

Schließen Sie spätestens jetzt alle offenen Anwendungen in Ihrem Windows-System, da diese sonst zu Problemen bei der Installation führen können. Lesen Sie sich nun die Lizenzvereinbarung zur Nutzung dieser Software durch. Wählen Sie **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** und klicken dann auf **Weiter**, wenn Sie den Vereinbarungen in dieser Form zustimmen. Der nächste Bildschirm ermöglicht Ihnen die Auswahl des Installationsordners.

Server-Typ auswählen

Sie haben bei der Auswahl der Server-Typen folgende Optionen:

- **Einen Main-Server installieren:** Bei einer Erstinstallation muss der G Data ManagementServer immer als **Main-Server (Main-MMS)** installiert werden. Der Main-Server stellt die zentrale Konfigurations- und Verwaltungsinstanz der netzwerkbasieren Virenschutz-Architektur dar. Die zu schützenden Rechner werden über den G Data ManagementServer mit den jeweils aktuellsten Virensignatur- und Programmupdates versorgt. Darüber hinaus werden sämtliche Client-Einstellungen zentral am G Data ManagementServer vorgenommen.
- **Einen Secondary-Server installieren:** Bei Verwendung einer **SQL-Datenbank** ist es möglich, einen **zweiten Server (Secondary-MMS)** zu betreiben, der auf die gleiche Datenbank wie der Hauptserver zugreift. Falls der **Main-Server** eine Stunde oder länger nicht erreichbar ist, werden die Clients sich automatisch mit dem Secondary-Server verbinden und von diesem Signaturupdates laden. Der Wechsel zurück zum Hauptserver erfolgt, sobald dieser wieder verfügbar ist. Beide Server laden die Signaturupdates unabhängig voneinander und stellen so eine Ausfallsicherheit her.
- **Einen Subnet-Server installieren:** Bei großen Netzwerken (z.B. Firmenzentrale mit angeschlossenen Zweigstellen) kann es sinnvoll sein, einen G Data ManagementServer als **Subnet-Server** zu betreiben. Subnet-Server dienen der Entlastung des Netzwerks zwischen Clients und dem Main-MMS. Sie können in Netzwerken verwendet werden und verwalten dort die ihnen zugeordneten Clients. Die Subnet-Server bleiben funktionsfähig, auch wenn Main- oder Secondary-ManagementServer nicht erreichbar sind. Diese laden allerdings selbständig keine Virensignaturupdates.

Schematisch sähe ein **Aufbau der Server-Typen** in großen Netzwerken folgendermaßen aus: Subnet-Server bündeln die Anfragen und Meldungen einzelner Clients oder Client-Gruppen und geben sie an den Main-Server weiter. Dieser wird von einem Secondary-Server unterstützt, der die Ausfallsicherheit sicherstellt.

Auswahl Datenbank

Wählen Sie nun eine Datenbank aus, die der G Data ManagementServer verwenden soll. Sie haben dabei die Möglichkeit, eine vorhandene **SQL-Server-Instanz** oder **Microsoft SQL-Express** zu verwenden.

Ein Server-Betriebssystem ist nicht zwingend erforderlich. Die **SQL**-Variante bietet sich vor allem in größeren Netzwerken mit einer Client-Anzahl **ab 1000** an.

Die **SQL Express**- Variante bietet sich in Netzwerken mit einer Client-Anzahl **bis 1000** an.

Computername

Überprüfen Sie nun den **Namen** des Rechners, auf dem der G Data ManagementServer installiert wird. Dieser Rechner muss über den hier angegebenen Namen von den Clients im Netzwerk angesprochen werden können. Sollte hier nicht der korrekte Name angezeigt werden, ändern Sie die Angabe unter **Name** entsprechend.

Produktaktivierung

Während der Installation erfolgt die **Produktaktivierung**. Diese ermöglicht das Laden von Updates nach Beendigung der Installation.

- **Registriernummer eingeben:** Wenn Sie die G Data Software das erste Mal installieren, wählen Sie diese Option aus und geben anschließend die Registriernummer ein, die dem Produkt beiliegt. Sie finden diese je nach Art des Produktes auf der Lizenzurkunde (MediaPack) oder in der Auftragsbestätigung. Kontaktieren Sie im Zweifelsfall Ihren Händler bzw. den betreuenden Distributor.

Durch die Eingabe der Registrierungsnummer wird Ihr Produkt aktiviert. Die erstellten Zugangsdaten werden Ihnen nach erfolgreicher Registrierung angezeigt. **Notieren Sie sich unbedingt diese Zugangsdaten!** Nach erfolgter Registrierung ist eine erneute Eingabe des Lizenzschlüssels nicht mehr möglich.

Sollten Sie bei der Eingabe der Registriernummer Probleme haben, überprüfen Sie die Registriernummer auf die korrekte Eingabe. Je nach verwendeten Schriftsatz wird ein großes "I" (wie Ida) oft als die Ziffer "1", bzw. dem Buchstaben "l" (wie Ludwig) fehlinterpretiert. Das Gleiche gilt für: "B" und "8", "G" und 6, "Z" und "2".

- **Zugangsdaten eingeben:** Wenn die G Data Software schon einmal installiert wurde, haben Sie Zugangsdaten (**Benutzername** & **Passwort**) erhalten. Um die G Data Software erneut zu installieren, geben Sie hier die Zugangsdaten an.

Dem Produkt liegen beim Neuerwerb keine Zugangsdaten bei!

- **Später aktivieren:** Wenn Sie sich zunächst nur einen Überblick über die Software verschaffen möchten oder die Zugangsdaten für den Moment nicht greifbar sind, kann die Installation auch ohne Angabe von Daten installiert werden. Da auf diese Weise allerdings vom Programm keine Aktualisierungen aus dem Internet geladen werden, ist kein echter Schutz vor Schadsoftware gegeben. Sie können Ihre Registrierungsnummer oder Ihre Zugangsdaten jederzeit nachträglich eingeben, sobald Sie ein Update durchführen. Beachten Sie: wird die Software installiert, ohne sie zu aktivieren, sind nur die G Data AntiVirus-Komponenten verfügbar, selbst wenn Sie eine G Data ClientSecurity, eine G Data EndpointProtection oder andere Module erworben haben. Die zusätzlichen Komponenten werden aktiviert und sind verfügbar, sobald die Software registriert wird. Lesen Sie hierzu auch die **Hinweise zur nachträglichen Aktivierung der G Data Software**.

Nur mit tagesaktuellen Updates kann die G Data Software Ihren Computer effektiv schützen. Eine Nutzung der Software ohne Aktivierung schützt Sie nur unzureichend.

Konfiguration Datenbanktyp

Dieser Installationsschritt erfolgt nur dann, wenn Sie den G Data ManagementServer neu installieren oder auf dem Rechner noch eine **SQL-Datenbank** vorinstalliert ist. In der Regel reicht es, diese Info-Box durch Anklicken der Schließen-Schaltfläche zu schließen.

Installationsabschluss

Nach der Installation des G Data ManagementServers ist dieser einsatzbereit. Um Änderungen an Clienteinstellungen vorzunehmen, können Sie unter **Start > (Alle) Programme > G Data Administrator** den Eintrag **G Data Administrator** auswählen und auf diese Weise das Administrationstool für den G Data ManagementServer starten. Der G Data ManagementServer wird bei jedem System(neu)start automatisch mitgestartet.

3.2 G Data Administrator



Bei einer Installation des **G Data ManagementServers** wird automatisch auf demselben Rechner der **G Data Administrator** mitinstalliert. Eine nachträgliche Installation der Administratorsoftware auf dem G Data ManagementServer ist nicht erforderlich.

Die Installation des G Data Administrators kann unabhängig von der Installation auf dem Server auch auf jedem Client-Rechner erfolgen.

Auf diese Weise kann der G Data ManagementServer auch dezentral betreut werden. Zur Installation des G Data Administrators auf einem Client-Rechner legen Sie die G Data-DVD in das DVD-Laufwerk des Client-Rechners und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend die Komponente **G Data Administrator** durch einen Klick auf die nebenstehende Schaltfläche.

Schließen Sie spätestens jetzt alle offenen Anwendungen im Windows-System, da diese sonst zu Problemen bei der Installation führen können. Nach einem Klick auf **Weiter** wird die Installation fortgesetzt; folgen Sie dann den Installationsschritten, bei denen der Installationsassistent Sie unterstützt. Nach der Installation ist unter **Start > (Alle) Programme > G Data Administrator** der Eintrag **G Data Administrator** anwählbar.

Anmeldung

Beim Starten des G Data Administrators werden Sie nach dem **Server, Authentisierung, Benutzername** und **Kennwort** gefragt. Geben Sie in dem Feld **Server**, den Namen des Computers ein, auf dem der G Data ManagementServer installiert wurde. Wählen Sie nun Ihre **Authentisierung** aus.

- **Windows-Authentisierung:** Wenn Sie diese Authentisierungsvariante wählen, können Sie sich mit dem Benutzernamen und Passwort Ihres Windows-Administrator-Zugangs auf dem G Data ManagementServer einloggen.
- **Integrierte Authentisierung:** Mit der integrierten Authentisierung können Sie als Systemadministrator auch anderen Personen Zugriff auf den G Data Administrator geben. So können Sie z.B. ein spezielles Konto anlegen, das nur Leserechte beinhaltet. Diese zusätzlichen Konten können Sie über die Funktion **Benutzerverwaltung** anlegen und verwalten.

Einrichtungsassistent

Beim ersten Start des G Data Administrators wird automatisch der **Einrichtungsassistent** geöffnet. Dieser hilft bei der Einrichtung der Clients und führt Sie durch alle wesentlichen Einstellungen. Der Assistent kann auch nach der Erstinstallation über den Befehl **Einrichtungsassistent** im **Admin**-Menü jederzeit nachträglich gestartet werden.

Weitere Programmstarts

Sie können den G Data Administrator zur Steuerung des G Data ManagementServers mit einem Klick auf den Eintrag **G Data Administrator** in der Programmgruppe **G Data** des Startmenüs aufrufen. Beim Starten des G Data Administrators werden Sie nach dem Server und dem Kennwort gefragt. Geben Sie in dem Feld **Server**, den Namen des Computers ein, auf dem der G Data ManagementServer installiert wurde. Nun öffnet sich die Programmoberfläche des Administrators.

3.3 G Data WebAdministrator



Bei der Installation des G Data WebAdministrators werden Sie ggf. dazu aufgefordert, **Microsoft .NET Framework-Komponenten** zu installieren. Diese sind zum Betrieb des G Data WebAdministrators unverzichtbar. Nach der Installation ist ein Neustart erforderlich.

Achtung: VOR der Installation des G Data WebAdministrators ist die Aktivierung der Windows-Funktion **Kompatibilität mit IIS-Metabasis und IIS 6-Konfiguration** erforderlich. Sollte diese Funktion nicht zur Verfügung stehen, wird die Installation des G Data WebAdministrators abgebrochen. Sie finden diesen Eintrag z.B. bei Windows Vista unter **Start > Systemsteuerung > Programme > Programme und Funktionen > Windows-Funktionen ein- oder ausschalten**. Hier können Sie den Eintrag unter **Internetinformationsdienste > Webverwaltungstools > Kompatibilität mit der IIS 6-Verwaltung > Kompatibilität mit IIS-Metabasis und IIS 6-Konfiguration** an- oder ausschalten. Außerdem müssen - soweit nicht schon geschehen - die **WWW-Dienste** aktiviert sein. Hierzu setzen Sie das Häkchen unter **Internetinformationsdienste > WWW-Dienste**.

In Serverbetriebssystemen finden sich die entsprechenden Optionen im Servermanager bei **Rollen**.

Der G Data WebAdministrator benötigt Microsoft Silverlight. Falls dies bei der Installation nicht vorhanden ist, werden Sie beim ersten Start des G Data WebAdministrators darauf aufmerksam gemacht. Eine nachträgliche Installation von Silverlight ist möglich.

Nun können Sie den G Data WebAdministrator installieren.



Nach der Installation steht Ihnen auf dem Desktop Ihres Computers das Symbol für den **G Data WebAdministrator** zur Verfügung.

3.4 G Data Security Clients

Sollte die Installation der Clients über das Netzwerk fehlschlagen, kann die Client-Software auch direkt auf den Client-Rechnern installiert werden. Prüfen Sie jedoch zuvor die **Voraussetzungen für die Remote-Installation**. Zur lokalen Installation des Clients auf einem Client-Rechner legen Sie die G Data-DVD in das DVD-Laufwerk des Client-Rechners ein und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend die Komponente **G Data Security Client** durch einen Klick auf die nebenstehende Schaltfläche. Geben Sie im Verlauf der Installation den **Servernamen** oder die **IP-Adresse des Servers** ein, auf dem der G Data ManagementServer installiert ist. Die Angabe des Servernamens ist notwendig, damit der Client über das Netzwerk mit dem Server in Kontakt treten kann. Außerdem muss der **Computername** dieses Rechners eingegeben werden, soweit dieser nicht automatisch angezeigt wird.

Zur Installation von Clients für Samba-Fileserver lesen Sie im Anhang dieser Dokumentation das Kapitel: **Installation des Clients für Samba-Fileserver**.

Hinweis für Nutzer der SmallBusiness Security: Wenn Sie über Rechner verfügen, die aus unterschiedlichen Gründen nicht mit dem G Data Security Client bestückt werden sollen, können Sie diese mit der G Data InternetSecurity-Software bespielen. Diese Software bietet diesen Rechnern unabhängig vom Server einen gewohnt zuverlässigen G Data Schutz. Wie Sie die Software installieren und verwenden, finden Sie in der Hilfedokumentation, die der Software online beiliegt.

3.5 G Data MailSecurity

Vor der Installation sollten Sie sich Gedanken darüber machen, wo im Netzwerk Sie *G Data MailSecurity* installieren. Während Sie die *G Data MailSecurity-Administratorsoftware* von jedem Punkt des Netzwerks aus verwenden können, benötigt die Installation des eigentlichen MailGateways einiger Vorüberlegungen. Generell sollte sich das MailGateway am besten direkt hinter Ihrer Netzwerk-Firewall befinden (soweit vorhanden), d.h. dass der SMTP/POP3-Datenstrom aus dem Internet über die **Firewall** direkt zum MailGateway geleitet und von dort weiter verteilt wird.

Bitte beachten Sie, dass Sie gegebenenfalls Ihre **Firewall-Konfigurationen** (IP-Adresse und/oder Port) verändern müssen, damit der E-Mailverkehr über das *G Data MailSecurity MailGateway* abgewickelt wird.

Prinzipiell können Sie das *G Data MailSecurity MailGateway* auf einem eigenen Rechner installieren, der dann für das gesamte Netzwerk als MailGateway fungiert, es ist aber auch möglich, *G Data MailSecurity* auf dem Rechner einzusetzen, der gleichzeitig als Mail-Server dient. Dabei ist zu beachten, dass eine gemeinsame Installation auf einem einzigen Rechner bei starkem Mail-Aufkommen zu Verzögerungen führen kann, da sowohl die Verwaltung permanenter E-Mail-Kommunikation, als auch die immanenten Virenanalyse sehr rechenintensive Vorgänge sind.

Installation des MailGateways auf dem Mail-Server (SMTP)

Wenn Ihr **SMTP-Server** die Änderung der Port-Nummer erlaubt, können Sie *G Data MailSecurity* auch auf demselben Rechner installieren, wie Ihren SMTP-Server. In diesem Fall vergeben Sie bitte für Ihren Original-Mail-Server eine neue Port-Nummer (z.B. 7100 oder höher). Das *MailGateway* verwendet dann weiterhin **Port 25** zur Verarbeitung eingehender Mails.

Sollten Sie *G Data MailSecurity* auf demselben Rechner wie **Microsoft Exchange 5.5** installieren, kann das *G Data MailSecurity Setup* automatisch den Port für eingehende Mails umstellen. Dazu wird der SMTP-Eintrag in der Datei **\winnt\system32\drivers\etc\services** verändert und der Internet Mail Dienst von Microsoft Exchange neu gestartet. Beispiel:

Configuration Mail-Server

Port für eingehende Mails: 7100 (Beispiel)

Nachrichtenübermittlung: Alle Nachrichten zum Host weiterleiten: 127.0.0.1

Konfiguration G Data MailSecurity MailGateway (Eingehend (SMTP))

Port, auf dem die Mails eingehen: 25

DNS zum Versenden der Mails verwenden: AUS

Mails an diesen SMTP-Server weiterleiten: 127.0.0.1

Port: 7100 (Beispiel)

Konfiguration G Data MailSecurity MailGateway (Ausgehend (SMTP))

Ausgehende Mail verarbeiten: EIN

IP-Adressen der Server, die ausgehende Mails senden können: 127.0.0.1;<IP Mail-Server>

DNS zum Versenden der Mails verwenden: EIN

Bezeichnungen

<IP Mail-Server> = IP-Adresse des Rechners, auf dem der Mail-Server installiert ist.

<IP G Data MailSecurity> = IP-Adresse des Rechners, auf dem G Data MailSecurity installiert ist.

Installation des MailGateways auf separatem Rechner (SMTP)

Hierbei müssen eingehende Mails an das *G Data MailSecurity MailGateway* gesendet werden (nicht an den Mail-Server). Das kann über unterschiedliche Methoden erreicht werden:

- a) den **MX-Record** im **DNS-Eintrag** anpassen
- b) Umleitung an der **Firewall** definieren (falls vorhanden)
- c) die **IP-Adresse** des Mail-Servers ändern und dem Rechner mit dem *G Data MailSecurity MailGateway* die originale IP-Adresse des Mail-Servers zuweisen

Konfiguration Mail-Server

Port für eingehende Mails: 25

Nachrichtenübermittlung: Alle Nachrichten zum Host weiterleiten: <IP G Data MailSecurity>

Konfiguration G Data MailSecurity MailGateway (Eingehend (SMTP))

Port, auf dem die Mails eingehen: 25

DNS zum Versenden der Mails verwenden: AUS

Mails an diesen SMTP-Server weiterleiten: <IP Mail-Server>

Port: 25

Konfiguration G Data MailSecurity MailGateway (Ausgehend (SMTP))

Ausgehende Mail verarbeiten: EIN

IP-Adressen der Server, die ausgehende Mails senden können: <IP Mail-Server>

DNS zum Versenden der Mails verwenden: EIN

Bezeichnungen

<IP Mail-Server> = IP-Adresse des Rechners, auf dem der Mail-Server installiert ist.

<IP G Data MailSecurity> = IP-Adresse des Rechners, auf dem das G Data MailSecurity MailGateway installiert ist

Installationsvorgang

Schließen Sie bitte alle anderen Programme, bevor Sie mit der Installation von *G Data MailSecurity* beginnen. Es kann zu Fehlfunktionen oder einem Abbruch kommen, falls z.B. Programme geöffnet sind, die auf Daten zugreifen, die *G Data MailSecurity* zur Installation benötigt. Beachten Sie bitte auch, dass für eine Installation ausreichender Festplattenspeicherplatz auf Ihrem System zur Verfügung steht. Sollte während der Installation nicht genügend Speicherplatz zur Verfügung stehen, weist Sie das Installationsprogramm von *G Data MailSecurity* darauf hin. Die Installation von *G Data MailSecurity* ist ausgesprochen unkompliziert. Starten Sie einfach Ihr Windows und legen dann die *G Data MailSecurity-CD-ROM* in Ihr CD-ROM-Laufwerk ein. Es öffnet sich automatisch ein Installationsfenster, welches Ihnen folgende Optionen bietet:

- **Installieren:** Hiermit starten Sie die Installation von *G Data MailSecurity* auf Ihrem Computer.
- **Durchsuchen:** Über den Windows-Explorer können Sie hier die Verzeichnisse der *G Data MailSecurity-CD-ROM* sichten.

- **Abbrechen:** Über diesen Eintrag können Sie die den Autostart-Bildschirm schließen, ohne eine Aktion durchzuführen.

Sollten Sie die **Autostart-Funktion Ihres CD-ROM-Laufwerks** nicht aktiviert haben, kann *G Data MailSecurity* den Installationsvorgang nicht automatisch starten. Klicken Sie dann im **Start-Menü** von Windows auf **Ausführen**, tippen in dem erscheinenden Fenster **e:** \setup.exe ein und klicken auf **OK**. Auf diese Weise öffnet sich ebenfalls der Einstiegsbildschirm für die *G Data MailSecurity-Installation*. Der Eintrag **e:** bezeichnet den Laufwerksbuchstaben Ihres CD-ROM-Laufwerks. Sollten Sie Ihr CD-ROM-Laufwerk auf einem anderen Laufwerksbuchstaben angemeldet haben, geben Sie statt **e:** bitte den entsprechenden Laufwerksbuchstaben an.

Folgen Sie nun einfach den einzelnen Schritten des Installationsassistenten und installieren Sie über die Schaltfläche **G Data MailSecurity** das MailGateway auf dem Rechner, den Sie dafür verwenden möchten. Das kann im besten Fall ein speziell dafür abgestellter MailGateway-Rechner sein, aber auch der Mail-Server-Rechner selber bzw. irgendein anderer Computer, der im Netzwerk administrative Aufgaben übernehmen kann. Bitte beachten Sie in diesem Zusammenhang die **Mindestsystemvoraussetzungen**, die für den Betrieb des MailGateways notwendig sind.

Über den Installationsabschnitt **E-Mail-Statistik** können Sie eine statistische Auswertung des E-Mail-Verkehrs auf dem Mailserver mitinstallieren. Wenn Sie diese Option verwenden, finden Sie im **Optionen**-Menü des Administrators eine zusätzliche Registerkarte namens **Datenbank**.

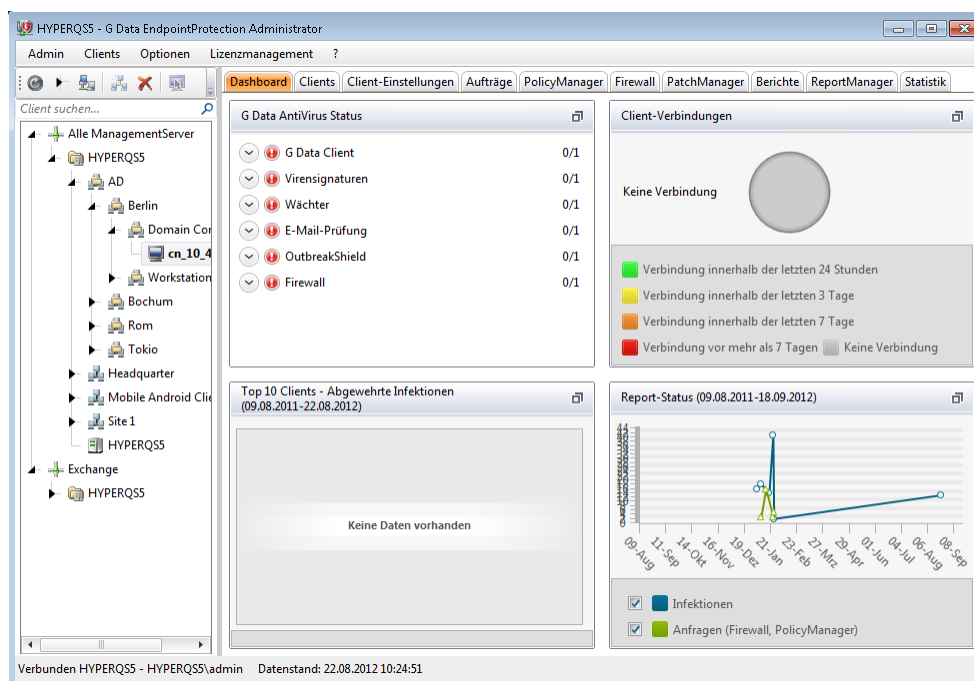
4 G Data ManagementServer

Der **G Data ManagementServer** ist das Herzstück der G Data Architektur: Er verwaltet die Clients, fordert neueste Software- und Virensignaturupdates automatisch vom G Data UpdateServer an und steuert den Virenschutz im Netzwerk. Zur Kommunikation mit den Clients nutzt der G Data ManagementServer das **TCP/IP**-Protokoll. Für **Clients**, die vorübergehend keine Verbindung zum G Data ManagementServer haben, werden die Jobs automatisch gesammelt und beim nächsten Kontakt zwischen G Data Security Client und G Data ManagementServer synchronisiert. Der G Data ManagementServer verfügt über einen zentralen **Quarantäne**-Ordner. In diesem können verdächtige Dateien verschlüsselt sichergestellt, gelöscht, desinfiziert oder gegebenenfalls an die **Internet-Ambulanz** weitergeleitet werden. Der G Data ManagementServer wird über den **G Data Administrator** gesteuert.

Wenn Sie den G Data Administrator beenden, bleibt der G Data ManagementServer weiterhin im Hintergrund aktiv und steuert die Prozesse, die von Ihnen für die Clients eingestellt wurden.

5 G Data Administrator

Der **G Data Administrator** ist die Steuerungssoftware für den G Data ManagementServer, die die Verwaltung von Einstellungen und Updates für alle im Netzwerk installierten G Data-Clients ermöglicht. Der G Data Administrator ist passwortgeschützt und kann auf jedem Windows-Rechner innerhalb des Netzwerkes installiert und gestartet werden. Im G Data Administrator lassen sich Scanaufträge und Wächterfunktionen sowie Änderungen von Einstellungen vornehmen. Automatische Clientinstallationen, Software- und Virensignaturupdates, werden ebenfalls dort festgelegt. Das Administrator-Tool zur Steuerung des G Data ManagementServers wird mit einem Klick auf den Eintrag **G Data Administrator** in der Programmgruppe **Start > (Alle) Programme > G Data Administrator** des Startmenüs aufgerufen.



Die Oberfläche des G Data Administrators ist in folgende Bereiche untergliedert:

- Der links befindliche **Clientauswahlbereich** zeigt alle Clients, auf denen die G Data Clientsoftware installiert ist.
- Rechts davon kann über Karteireiter in die jeweiligen **Aufgabenbereiche** gewechselt werden. Der Inhalt des Aufgabenbereiches bezieht sich normalerweise auf den im Clientauswahlbereich markierten Computer bzw. auf die markierte Gruppe von Clients.
- Oberhalb dieser Spalten finden Sie eine **Menüleiste** für globale Funktionen, die in allen Aufgabenbereichen verwendet werden können, sowie Sonderfunktionen für ausgewählte Aufgabenbereiche.

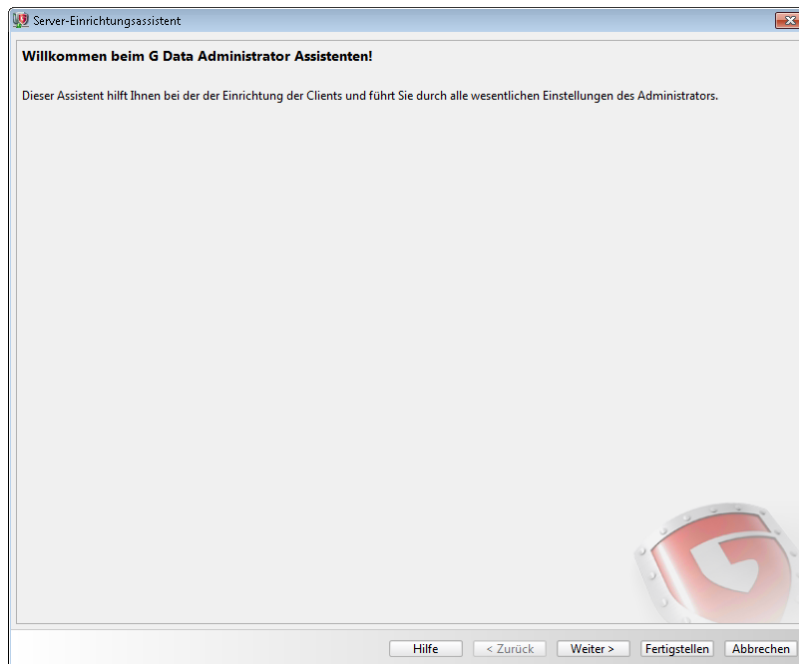
Bei der Administration von **Linux-Clients**, die auf **Samba-Servern** installiert sind, sind Funktionen, die z.B. den Umgang mit E-Mails beinhalten, gesperrt, da diese im Kontext eines Fileservers nicht notwendig sind. Funktionen, die für Linux-Clients nicht einstellbar sind, werden durch ein rotes Ausrufezeichen vor der jeweiligen Funktion markiert.

5.1 Menüleiste

Admin

Server-Einrichtungsassistent

Mit dem Einrichtungsassistenten lassen sich im Netzwerk die Clients auswählen und aktivieren, für die die G Data Software den Virenschutz bereitstellen soll.



Aktivieren

Zunächst müssen alle Clients, die von der G Data Software überwacht werden sollen, aktiviert werden. Die zu aktivierenden Clients müssen zunächst markiert und mit einem Klick auf **Aktivieren** aktiviert werden. Eventuell sind einige Computer nicht in der Liste enthalten (z.B. weil die betreffenden Rechner lange nicht eingeschaltet waren oder keine Datei- bzw. Druckerfreigabe eingerichtet haben). Zum Aktivieren dieser Clients wird im Eingabefeld **Computer** der Name des Rechners eingegeben. Nach einem Klick auf **Aktivieren** wird der zu aktivierende Rechner in die Clientliste aufgenommen. Wenn alle zu schützenden Rechner aktiviert wurden, folgt nach einem Klick auf **Weiter** der nächste Schritt.

Installieren

Im folgenden Dialog ist das Häkchen bei **Client-Software automatisch auf den aktivierten Computern installieren** voreingestellt. Wenn die Verteilung der Software auf den Client-Rechnern zu einem späteren Zeitpunkt erfolgen soll, muss diese Option durch Entfernen des Häkchens deaktiviert werden.

Internet-Update

Der G Data ManagementServer lädt über das Internet neue Virensignaturen und Programmdateien herunter. Damit dieser Vorgang automatisch erfolgen kann, ist die Eingabe der **Zugangsdaten** erforderlich, die bei der Online-Registrierung erstellt wurden. Eine detaillierte Beschreibung zur Planung von Updateintervallen finden Sie im Kapitel **Internet-Update**. Es besteht auch die Möglichkeit, das Internet-Update nachträglich über die G Data Administrator-Programmoberfläche zu automatisieren.

E-Mail-Benachrichtigung

Im Fall eines Virenfundes auf einem oder mehreren Clients oder bei anderen kritischen Situationen kann der Netzwerkadministrator per Mail informiert werden. Geben Sie dazu die E-Mail-Adresse des Empfängers der Warnmeldungen an. Über die **Begrenzung** lässt sich ein übermäßiges Mailaufkommen im Fall eines massiven Virenbefalls verhindern. Mit **Fertigstellen** wird der Assistent beendet.

Automatische Installation der Client-Software

Wenn bei der Einrichtung festgelegt wurde, dass die Client-Software automatisch installiert werden soll, erfolgt eine Abfrage von Zugangsdaten für ein Benutzerkonto, das über administrative Rechte auf dem Zielsystem verfügt. Nach der Bestätigung des Dialogs versucht der G Data ManagementServer die Client-Software auf allen aktivierten Computern zu installieren. Ein Info-Bildschirm informiert dabei über den Fortschritt der Installation und eventuelle Probleme.

Abhängig davon, welche Produktversion eingesetzt wird, können Sie hier auch festlegen, dass auf den Client-PCs die **G Data Firewall** mitinstalliert wird. Die Firewall ist nur in der **G Data ClientSecurity**, der **G Data EndpointProtection** und der **G Data SmallBusiness Security** verfügbar.

Sollte es Probleme bei der **Remote-Installation** der G Data Clients über den G Data Administrator geben, besteht auch die Möglichkeit, die Client-Software mittels der G Data DVD oder mit Hilfe eines selbst erstellten Client-Installationspaketes auf den Clientrechnern zu installieren. Lesen Sie hierzu auch das Kapitel **G Data Client installieren**.

Eine spezielle Client-Software für **Linux-Clients** ist verfügbar. Lesen Sie hierzu das Kapitel **Installation der Client-Software auf Linux-Rechnern** im Anhang dieser Dokumentation.

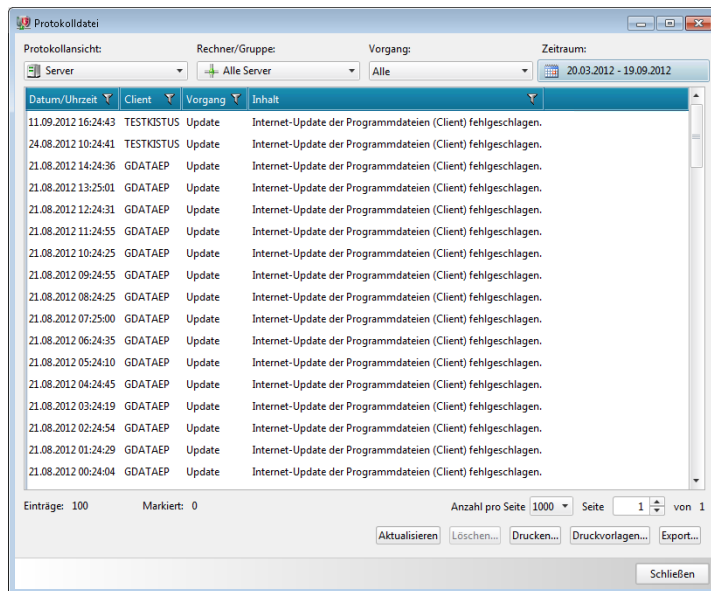
Siehe hierzu auch: **G Data Security Client installieren**

Protokoll anzeigen

In der **Protokolldatei** steht ein Überblick über die letzten von der G Data Software durchgeführten Aktionen zur Verfügung. Hier werden sämtliche relevanten Informationen angezeigt. Die Anzeige des Protokolls kann nach folgenden Kriterien gefiltert werden:

- **Protokollansicht:** Legen Sie hier fest, ob Sie ein Protokoll von den Client- oder Servervorgängen einsehen möchten.
- **Rechner/Gruppe:** Hier können Sie festlegen, ob Sie sich ein Protokoll aller Clients bzw. Gruppen oder nur einzelner Bereiche anschauen möchten.
- **Vorgang:** Definieren Sie hier, ob Sie alle protokollierten Informationen einsehen möchten oder nur Meldungen zu bestimmten Themen.
- **Zeitraum:** Hier können Sie den von/bis Zeitraum definieren, für den Protokollinformationen eingesehen werden sollen.

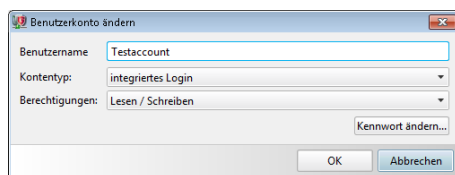
Das Feld **Aktualisieren** dient dazu, Vorgänge mit aufzulisten, die sich ereignen, während die Protokollansicht geöffnet ist. Sämtliche Vorgänge erscheinen erst einmal in chronologischer Reihenfolge und lassen sich durch einfaches Klicken auf die jeweilige Spaltenbezeichnung nach bestimmten Kriterien sortieren. Die Spalte, nach der die aktuelle Sortierung erfolgt, wird dabei durch ein kleines Pfeilsymbol gekennzeichnet.



Datum/Uhrzeit	Client	Vorgang	Inhalt
11.09.2012 16:24:43	TESTKISTUS	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.
24.08.2012 10:24:41	TESTKISTUS	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.
21.08.2012 14:24:36	GDATAEP	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.
21.08.2012 13:25:01	GDATAEP	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.
21.08.2012 12:24:31	GDATAEP	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.
21.08.2012 11:24:55	GDATAEP	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.
21.08.2012 10:24:25	GDATAEP	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.
21.08.2012 09:24:55	GDATAEP	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.
21.08.2012 08:24:25	GDATAEP	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.
21.08.2012 07:25:00	GDATAEP	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.
21.08.2012 06:24:35	GDATAEP	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.
21.08.2012 05:24:10	GDATAEP	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.
21.08.2012 04:24:45	GDATAEP	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.
21.08.2012 03:24:19	GDATAEP	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.
21.08.2012 02:24:54	GDATAEP	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.
21.08.2012 01:24:29	GDATAEP	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.
21.08.2012 00:24:04	GDATAEP	Update	Internet-Update der Programmdateien (Client) fehlgeschlagen.

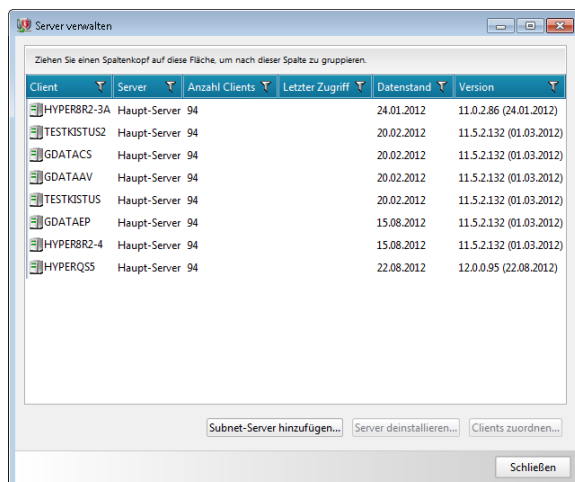
Benutzerverwaltung

Als Systemadministrator können Sie weitere Benutzerzugänge für das G Data Administrator-Interface vergeben. Klicken Sie dazu auf die **Neu**-Schaltfläche und geben anschließend den Benutzernamen, die **Berechtigungen** dieses Nutzers (**Lesen/Schreiben** bzw. **nur Lesen**) ein, definieren Sie den **Kontentyp** (**integriertes Login**, **Windows-Benutzer**, **Windows-Benutzergruppe**) und vergeben Sie ein **Kennwort** für diesen Benutzer.



Server verwalten

Über die Server-Verwaltung können Sie **Clients** einzelnen **Subnet-Servern** zuordnen, die dann die Kommunikation dieser Clients mit dem **Main-Server** bündeln und auf diese Weise die Netzwerknutzung optimieren. Über dieses Menü können Sie Subnet-Server installieren. Über die Schaltfläche **Clients zuordnen** können Sie vorhandene Clients den definierten Subnet-Servern zuordnen.



Client	Server	Anzahl Clients	Letzter Zugriff	Datenstand	Version
HYPERBR2-3A	Haupt-Server	94	24.01.2012	11.0.2.86 (24.01.2012)	
TESTKISTUS2	Haupt-Server	94	20.02.2012	11.5.2.132 (01.03.2012)	
GDATAACS	Haupt-Server	94	20.02.2012	11.5.2.132 (01.03.2012)	
GDATAAV	Haupt-Server	94	20.02.2012	11.5.2.132 (01.03.2012)	
TESTKISTUS	Haupt-Server	94	20.02.2012	11.5.2.132 (01.03.2012)	
GDATAEP	Haupt-Server	94	15.08.2012	11.5.2.132 (01.03.2012)	
HYPERBR2-4	Haupt-Server	94	15.08.2012	11.5.2.132 (01.03.2012)	
HYPERQSS	Haupt-Server	94	22.08.2012	12.0.0.95 (22.08.2012)	

Die Zuordnung der Clients zu Subnet-Servern ist unabhängig von der Gruppierung von Clients. Daher können Clients, die unterschiedlichen Subnet-Servern zugeordnet sind, dennoch in Gruppen unterteilt werden.

Subnet-Server-Synchronisation

Um eventuelle Änderungen auch außerhalb des regulären Kommunikationsintervalls von Server und Subnet-Server zu ermöglichen, kann die Subnet-Server-Synchronisation auch manuell angestoßen werden.

Beenden

Über diese Funktion wird der G Data Administrator geschlossen. Der G Data ManagementServer bleibt weiterhin gestartet und steuert den Virenschutz im Netzwerk gemäß der festgelegten Vorgaben.

Clients

Aktualisieren

Um Änderungen im Netzwerk zu verfolgen, die sich zu der Zeit ergeben, in der Sie den G Data Administrator nutzen, können Sie die **Aktualisieren**-Funktion verwenden.

Deaktivierte Clients anzeigen



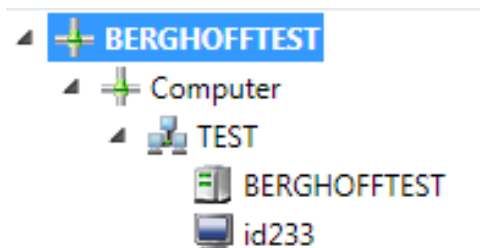
Clients, die nicht **aktiviert** sind, können über diese Funktion wieder sichtbar gemacht werden. **Deaktivierte Clients** werden dabei als durchscheinende Symbole dargestellt.



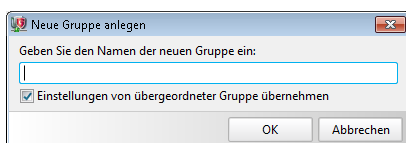
Im Gegensatz dazu sind **aktivierte Clients** durch vollfarbige Symbole gekennzeichnet.

Neue Gruppe anlegen

Über diesen Befehl lässt sich eine **Gruppe** anlegen. Clients können in Gruppen zusammengefasst und ihre Einstellungen gruppenweise festgelegt werden. Nach dem Anwählen dieser Option und der Vergabe eines Gruppennamens können Clients der neuen Gruppe zugeordnet werden.

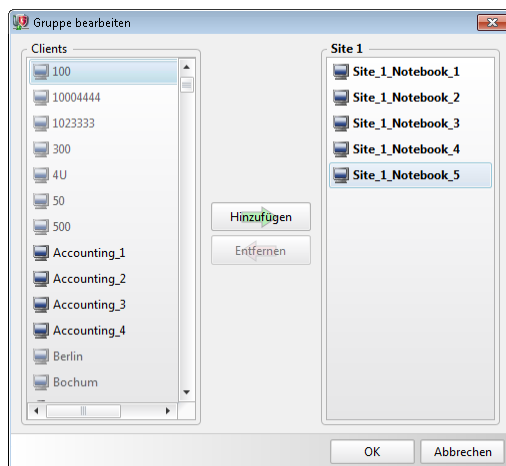


Clients können einer Gruppe zugeordnet werden, indem man in der Clientliste den gewünschten Client mit der Maus, per Drag&Drop, auf die entsprechende Gruppe zieht.



Gruppe bearbeiten

Diese Option öffnet eine Dialogbox, in der sich über die Tasten **Hinzufügen** und **Entfernen** Clients zur Gruppe hinzufügen oder aus der Gruppe entfernen lassen. Nur verfügbar, wenn im Clientauswahlbereich eine Gruppe angewählt ist.



Löschen

Einzelne Clients lassen sich mit dem Befehl **Löschen** aus der Clientliste entfernen. Durch das Entfernen des Clients aus der Liste wird der G Data Client nicht deinstalliert.

Um eine Gruppe zu löschen, müssen alle in ihr enthaltenen Clients nach Bedarf entweder deaktiviert oder in andere Gruppen verschoben werden. Nur leere Gruppen können gelöscht werden. Deaktivierte Clients lassen sich über die Funktion **Deaktivierte Clients anzeigen** wieder sichtbar machen.

G Data Client Installationspaket erstellen

Über diese Funktion ist es möglich, ein Installationspaket für den G Data Security Client zu erstellen. Das Paket ist eine einzelne ausführbare Datei (**GDClientPck.exe**), mit der ein neuer Client ohne weitere Benutzerinteraktion auf einem zu schützenden Rechner installiert werden kann. Das Installationspaket eignet sich beispielsweise dazu, den Client via Login-Script auf allen Rechnern einer Domäne zu verteilen.

Das Paket enthält immer die auf dem Server aktuelle Client-Version. Abhängig davon, welche Produktversion Sie verwenden, können Sie auf den Client-PCs die **G Data Firewall** per Remote-Installation nachinstallieren. Es ist unbedingt erforderlich, das Installationpaket auf den Zielrechner zu kopieren und dort mit Administratorrechten zu starten.

Optionen

Internet-Update

Hier werden alle Einstellungen für Internet-Updates der Virendatenbanken und der Programmdateien der G Data Software festgelegt. In der Karteikarte **Zugangsdaten und Einstellungen** sind die Zugangsdaten einzugeben, die bei der **Online-Registrierung** erstellt wurden. Beim Internet-Update werden die aktuellen Virendefinitionen vom G Data UpdateServer geladen und auf dem G Data ManagementServer gespeichert. Die Verteilung der Virensignaturen an die Clients wird vom Aufgabenbereich **Clients** gesteuert. Das Internet-Update stellt sicher, dass immer die aktuellen Virensignaturen und die neuesten Programmdateien vorhanden sind.

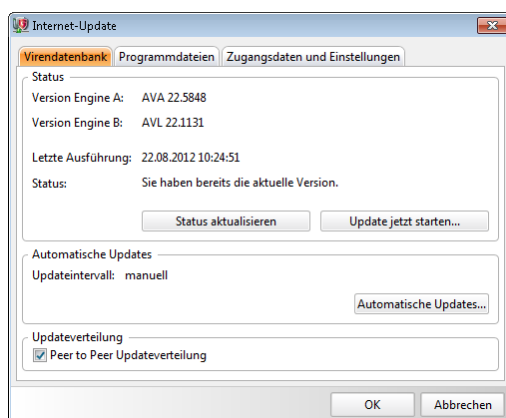
Virendatenbank

Alle Clients haben eine eigene, lokale Kopie der Virendatenbank, damit der Virenschutz auch gewährleistet ist, wenn sie offline sind (d.h. keine Verbindung mit dem G Data ManagementServer bzw. dem Internet besteht). Die **Aktualisierung** der Dateien auf den Clients erfolgt in zwei Schritten, die natürlich beide automatisiert werden können. Im ersten Schritt werden die aktuellen Dateien vom G Data UpdateServer in einen Ordner auf dem G Data ManagementServer kopiert. Im zweiten Schritt werden die neuen Dateien an die Clients verteilt (siehe Aufgabenbereich **Clients**).

- **Status aktualisieren:** Über diese Schaltfläche können Sie die Statusanzeige der Virensignaturen auf dem Client gegebenenfalls aktualisieren, falls Änderungen in der Anzeige noch nicht übernommen worden sind.
- **Update jetzt starten:** Über die Schaltfläche **Update jetzt starten** können Sie eine Aktualisierung der Virendatenbanken direkt durchführen. Dabei werden die aktuellen Virensignaturen heruntergeladen, die hinterher vom G Data ManagementServer an die Clients verteilt werden.
- **Automatische Updates:** Wie die Virenprüfungen können Sie auch die Internet-Updates automatisch durchführen lassen. Aktivieren Sie dazu das Häkchen bei **Update periodisch ausführen** und legen Sie fest, wann bzw. in welchem Turnus das Update zu erfolgen hat.

Damit das Update automatisch erfolgen kann, muss Ihr G Data ManagementServer mit dem Internet verbunden sein oder Sie der G Data Software eine automatische Einwahl ermöglichen. Geben Sie hierzu unter **Zugangsdaten und Einstellungen** gegebenenfalls **Benutzerkonto** und **Proxy-Einstellungen** vor.

- **Updateverteilung:** Die Verteilung kann zentral (MMS, SubnetServer > Clients) oder - wenn Sie das entsprechende Häkchenfeld aktivieren - auch dezentral (Peer to Peer) (MMS, SubnetServer, schon upgedatete Clients > Clients) erfolgen.



Programmdateien

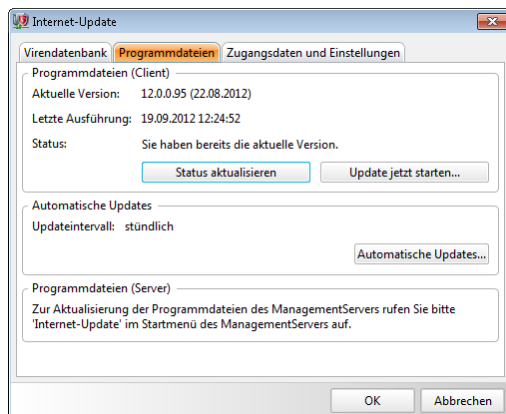
Wenn ein Programmupdate für die Client-Software von G Data bereit steht, können Sie die Aktualisierung der Clients über den G Data ManagementServer automatisch erledigen lassen. Die **Aktualisierung** der Dateien auf den Clients erfolgt in zwei Schritten, die beide automatisiert werden können. Im ersten Schritt werden die aktuellen Dateien vom G Data UpdateServer in einen Ordner auf dem G Data ManagementServer kopiert. Im zweiten Schritt werden die neuen Dateien an die Clients verteilt und damit wird der dortige Client aktualisiert (siehe **Aufgabenbereich Clients**).

- **Status aktualisieren:** Über die Schaltfläche **Aktualisieren** können Sie die Statusanzeige der Softwareversion auf dem Client gegebenenfalls aktualisieren, falls Änderungen in der Anzeige noch nicht übernommen worden sind.
- **Update jetzt starten:** Über die Schaltfläche **Update jetzt durchführen** können Sie eine Aktualisierung der Client-Software direkt durchführen. Dabei werden die aktuellen Clientdateien heruntergeladen, die hinterher vom G Data ManagementServer an die Clients verteilt werden.

- **Automatische Updates:** Wie die Virenprüfungen können Sie auch die Internet-Updates der Client-Software automatisch durchführen lassen. Aktivieren Sie dazu das Häkchen bei **Update periodisch ausführen** und legen Sie fest, wann bzw. in welchem Turnus das Update zu erfolgen hat.

Damit das Update automatisch erfolgen kann, muss der G Data ManagementServer mit dem Internet verbunden sein oder Sie der G Data Software eine automatische Einwahl ermöglichen. Geben Sie hierzu unter **Zugangsdaten und Einstellungen** gegebenenfalls **Benutzerkonto** und **Proxy-Einstellungen** vor.

Hinweis: Um die Programmdateien des G Data ManagementServers zu aktualisieren, rufen Sie in der Programmgruppe **G Data ManagementServer** im Startmenü den Eintrag **Internet-Update** auf. Der G Data ManagementServer kann ausschließlich über diesen Eintrag aktualisiert werden. Dagegen kann die G Data Client-Software auch über den G Data Administrator aktualisiert werden.



Zugangsdaten und Einstellungen

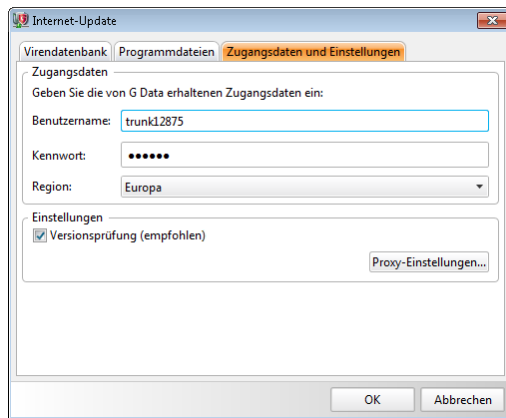
Mit der **Online-Registrierung** erhalten Sie von **G Data** die Zugangsdaten für das Update der Virendatenbanken und Programmdateien. Geben Sie diese unter **Benutzername** und **Kennwort** ein. Die (standardmäßig aktivierte) **Versionsprüfung** stellt bei jedem Internet-Update sicher, dass die aktuelle Virendatenbank kopiert, und die neuesten Programmdateien verwendet werden. Im Regelfall sollte die Versionsprüfung immer eingeschaltet sein, da sie den Download unnötig großer Updates verhindert. Sollten sich jedoch Probleme mit Virendatenbanken einstellen, dann schalten Sie Versionsprüfung aus. Auf diese Weise wird beim nächsten Internet-Update automatisch die aktuelle Version der Virendatenbank auf den Server überspielt. Mit der Schaltfläche **Proxy-Einstellungen** öffnen Sie ein Fenster, in dem Sie Zugangsdaten für Internet & Netzwerk eingeben können.

Achtung: Sie sollten hier nur Eingaben tätigen, wenn sich mit den Standardeinstellungen der G Data Software Probleme ergeben sollten (z.B. wegen der Verwendung eines **Proxyservers**) und ein Internet-Update nicht durchführbar ist.

Sie benötigen für Ihr Benutzerkonto die Informationen **Benutzername**, **Kennwort** und **Domäne**. Für die Anmeldung beim **Proxyserver** ist zusätzlich der Port (im Regelfall: 80) und - falls vom Benutzerkonto abweichend - eine Eingabe von Benutzername und Kennwort für den Proxyserver notwendig.

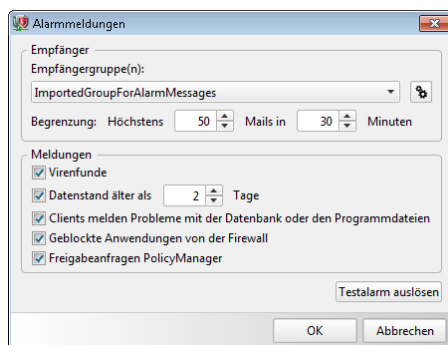
Benutzerkonto ist ein Konto für den Rechner, auf dem sich der ManagementServer befindet.

Die G Data Software kann die **Verbindungsdaten des Internet Explorer** (ab Version 4) verwenden. Konfigurieren Sie zunächst den **Internet Explorer** und prüfen Sie, ob die Testseite unseres Update-Servers erreichbar ist: <http://ieupdate.gdata.de/test.htm>. Schalten Sie anschließend die Option **Proxyserver verwenden** aus. Geben Sie unter **Benutzerkonto** das Konto ein, für den Sie den Internet Explorer konfiguriert haben (als das Konto, mit dem Sie sich an Ihrem Rechner angemeldet haben).

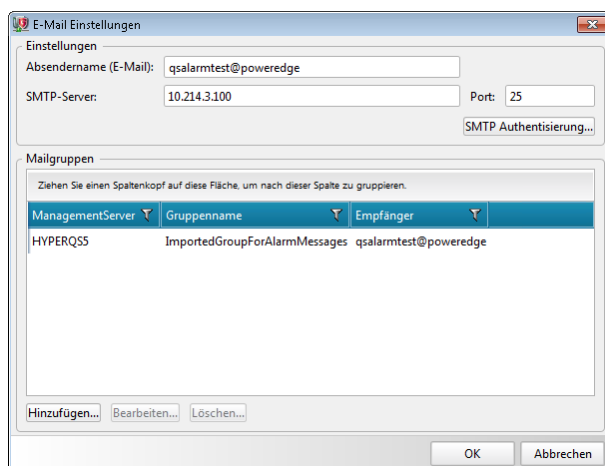


Alarmmeldungen

Bei neuen Virenfunden kann der G Data ManagementServer automatisch Alarmmeldungen per **E-Mail** versenden. Die dazu benötigten Einstellungen werden in diesem Bereich vorgenommen. Aktivieren Sie die E-Mail-Benachrichtigung, indem Sie das Häkchen bei den jeweils meldbaren Ereignissen setzen. Über die **Begrenzung** kann ein übermäßiges Mailaufkommen im Fall eines massiven Virenbefalls verhindert werden.



Um Änderungen an den E-Mail-Einstellungen vorzunehmen, klicken Sie bitte auf die Schaltfläche für erweiterte Einstellungen .



Geben Sie hier den Namen des Mailservers, den **SMTP-Server** und den **Port** (normalerweise 25) an. Weiterhin wird eine (gültige) Absenderadresse benötigt, damit die Mails verschickt werden können.

An diese E-Mail-Adresse werden auch die Antworten der **Internet-Ambulanz** geschickt.

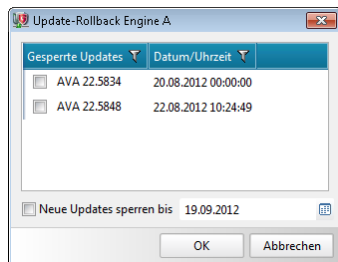
Unter **Mailgruppen** können Sie Listen verschiedener Empfänger und Empfängergruppen (z.B. Management, Techniker usw.) verwalten.

Update-Rollback Engine A / B

Es kann im seltenen Fall von Fehlalarmen oder ähnlichen Problemen sinnvoll sein, das aktuelle **Update der Virensignaturen** zu sperren und stattdessen eines der vorhergehenden Signaturupdates zu verwenden. Der G Data ManagementServer speichert von jeder AntiViren-Engine die letzten Updates. Sollte es also mit dem aktuellen Update der Engine A oder B Probleme geben, kann der Netzwerkadministrator das aktuelle Update für einen bestimmten Zeitraum sperren und stattdessen automatisch das zeitlich davorliegende Signaturupdate an die Clients und Subnet-Server verteilen.

Auf Clients, die nicht mit dem G Data ManagementServer verbunden sind (z.B. Notebooks auf Dienstreisen) können **keine** Rollbacks durchgeführt werden. Eine vom Server an den Client übertragene Sperrung neuer Updates kann dort ohne Kontakt zum G Data ManagementServer nicht rückgängig gemacht werden.

Die Anzahl der zu speichernden Rollbacks können Sie im Bereich **Server-Einstellungen** vornehmen. Standardmäßig werden die letzten fünf Signaturstände gespeichert.

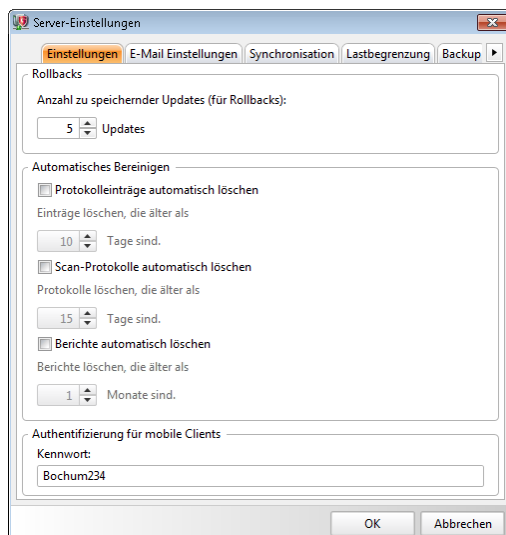


Server-Einstellungen

Einstellungen

Im Einstellungen-Bereich finden Sie folgende Optionen:

- **Rollbacks:** Geben Sie hier an, wie viele der aktualisierten Virensignaturupdates Sie für **Rollbacks** als Reserve vorhalten möchten. Als Standardwert gelten hier jeweils die letzten fünf Signaturupdates der jeweiligen Engine.
- **Automatisches Bereinigen:** Hier können Sie festlegen, dass **Protokolleinträge**, **Scan-Protokolle** und **Berichte** nach einem eingegebenen Zeitraum automatisch gelöscht werden.

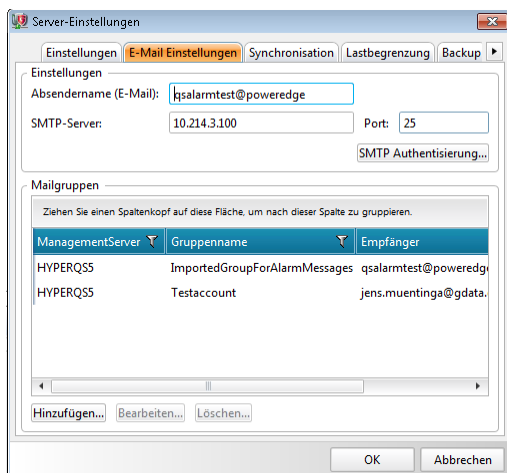


E-Mail-Einstellungen

Geben Sie hier den Namen des Mailservers, den **SMTP-Server** und den **Port** (normalerweise 25) an. Weiterhin wird eine (gültige) Absenderadresse benötigt, damit die Mails verschickt werden können.

An diese E-Mail-Adresse werden auch die Antworten der **Internet-Ambulanz** geschickt.

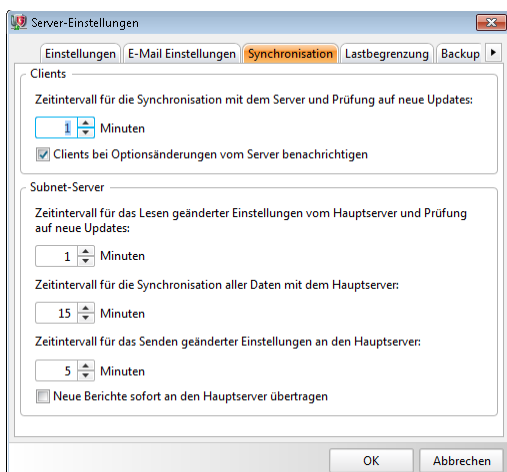
Unter **Mailgruppen** können Sie Listen verschiedener Empfänger verwalten.



Synchronisation

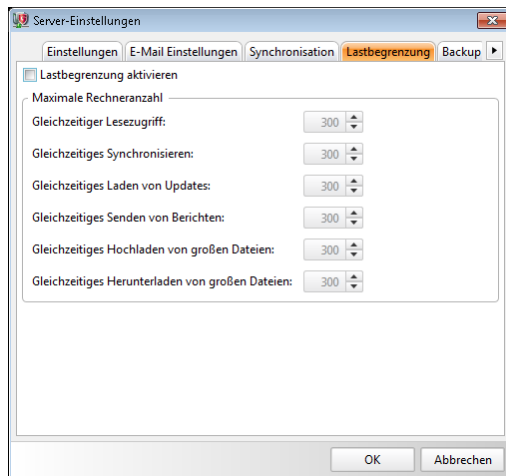
Im Synchronisation-Bereich können Sie das Synchronisationsintervall zwischen Clients, Subnet-Servern und Servern definieren:

- **Clients:** Geben Sie hier das Zeitintervall an, in dem die Clients mit dem Server synchronisiert werden. Wenn Sie das Häkchen bei **Clients bei Optionsänderungen vom Server benachrichtigen** setzen, erhält der Anwender auf dem Client-Rechner eine Meldung darüber, dass Änderungen vorgenommen wurden. Als Standardwert sind fünf Minuten festgelegt.
- **Subnet-Server:** Über diesen Bereich können Sie die Intervalle für die Kommunikation zwischen Server und Subnet-Server definieren. Wenn Sie das Häkchen bei **Neue Berichte sofort an den Hauptserver übertragen** setzen, dann werden Berichte unabhängig von den hier vorgenommenen Einstellungen sofort an den Hauptserver übertragen.



Lastbegrenzung

Wenn das Häkchen beim Eintrag **Lastbegrenzung aktivieren** gesetzt ist, lässt sich festlegen, wie viele Clients gleichzeitig die darunter aufgeführten Aktionen ausführen dürfen. So kann die Last verteilt werden, sodass es z.B. durch das gleichzeitige Laden von Updates zu keiner Latenzerhöhung im Netzwerk kommt.

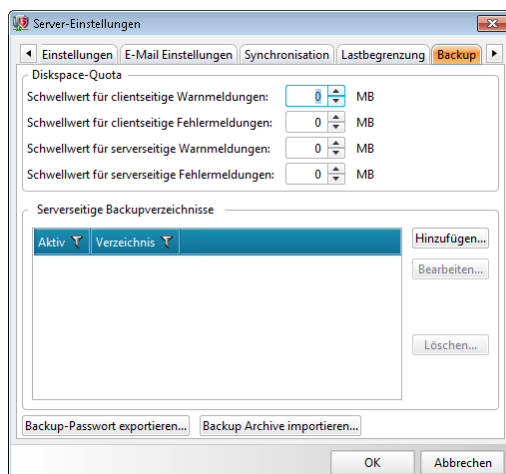


Backup

Im Bereich **Diskspace-Quota** werden Schwellenwerte für Warnungen eingestellt, die bei Erreichen der angegebenen Werte ausgegeben werden. Hier wird eingestellt, wie viel freier Speicherplatz auf dem Server frei sein muss, bevor eine Warnung oder eine Fehlermeldung ausgegeben wird. Dies ist sinnvoll, wenn beispielsweise für Anwendungen immer eine gewisse Menge Speicherplatz auf der Festplatte zur Verfügung stehen muss. Wird beispielsweise bei **Schwellwert für Clientseitige Warnmeldungen** der Wert 1500 angegeben, dann wird im G Data Administrator unter **Berichte** eine Warnung angezeigt, dass nur noch 1500 MB Speicherplatz verfügbar sind. Falls ein **Schwellwert für clientseitige Fehlermeldungen** angegeben wird, werden bei Erreichen des eingestellten Wertes ältere Backups gelöscht, um Speicherplatz für neue Backups zu schaffen. Dabei wird immer das älteste Backup zuerst gelöscht (FIFO-Prinzip).

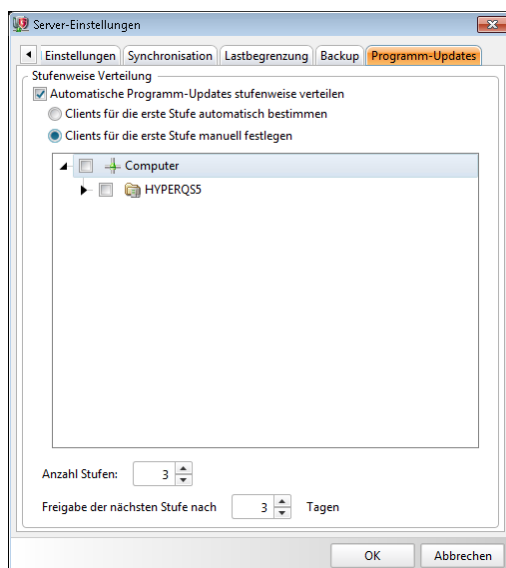
Darüber hinaus kann unter **Serverseitige Backupverzeichnisse** ein Pfad angegeben werden, auf dem alle auflaufenden Backups gespeichert werden sollen. Wird hier kein Verzeichnis angegeben, werden alle Backups unter **C:\ProgramData\G DATA\AntiVirus ManagementServer\Backup** bzw. **C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\G DATA\AntiVirus ManagementServer\Backup** gespeichert.

Da sämtliche mit der G Data Software erstellten Backups verschlüsselt sind, besteht auch die Möglichkeit, die Passwörter für die Backups zu exportieren und für eine spätere Verwendung zu speichern. Über die Schaltfläche **Backup Archive importieren** ermöglicht den Zugriff auf Backups, die in anderen Ordnern gespeichert sind.



Programm-Updates

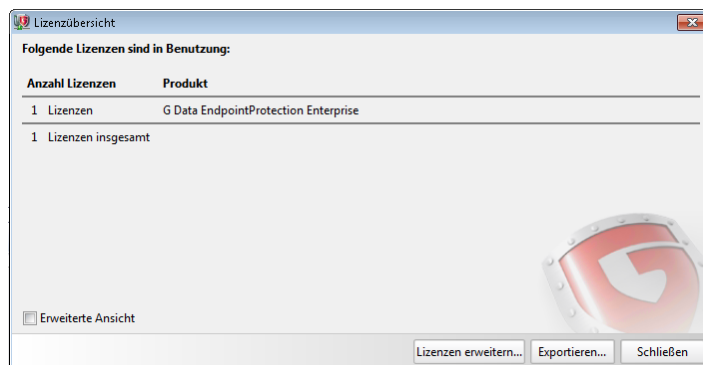
Im Bereich **Stufenweise Verteilung** können Sie festlegen, ob Sie Programmupdates zeitgleich auf allen Clients einspielen oder stufenweise. Eine stufenweise Verteilung verringert die Systemlast, die bei so einem Programmupdate unvermeidlich ist. Wenn Sie sich für eine stufenweise Verteilung entscheiden, können Sie festlegen, ob die Verteilung automatisch erfolgt oder selber festlegen, welche Clients zuerst mit Programm-Updates versehen werden sollen, welche Clients danach kommen und wie weit die Untergliederung in verschiedene Verteilungsstufen untergliedert ist.



Lizenzmanagement

Über das Lizenzmanagement haben Sie jederzeit Überblick darüber, wie viele Lizenzen Ihrer G Data Software in Ihrem Netzwerk installiert sind. Wenn Sie weitere Lizenzen benötigen, können Sie direkt über die Schaltfläche **Lizenzen erweitern** mit dem G Data Upgrade-Center Kontakt aufnehmen.

Über die Schaltfläche **Exportieren** haben Sie die Möglichkeit, sich eine Übersicht Ihrer verwendeten Lizenzen als Textdatei ausgeben zu lassen.



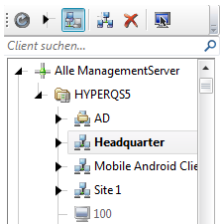
Wenn Sie hier das Häkchen bei **Erweiterte Ansicht** setzen, erhalten Sie die Information darüber, auf welchem Server explizit welche Lizenzen eingesetzt werden.

Hilfe

Hier erhalten Sie Informationen zum Programm und haben außerdem die Möglichkeit, auf die Online-Hilfe der G Data Software zurückzugreifen.

5.2 Clientauswahlbereich

Hier werden sämtliche Clients und Server sowie definierte Gruppen in Ihrem Netzwerk aufgelistet. Wie im Windows Explorer erscheinen Gruppen, in denen sich Untergliederungen befinden, mit einem kleinen Plus-Symbol. Wenn Sie dieses anklicken, öffnet sich die Verzeichnisstruktur an dieser Stelle und ermöglicht die Ansicht der darunter befindlichen Struktur.



Ein Klick auf das Minus-Symbol schließt diese Untergliederung wieder.

Active Directory Integration

Über die Active Directory-Integration können alle Computerobjekte der Organisationseinheiten der Domäne importiert werden. Dazu muss eine eigene Gruppe im G Data Administrator angelegt werden. Nach einem Rechtsklick auf die neu erstellte Gruppe wird der Menüpunkt **Active Directory Eintrag der Gruppe zuordnen** sichtbar.

Im Dialogfenster, das sich öffnet, wählen Sie den Punkt **Einer Gruppe im Active Directory zuweisen** aus und geben darunter den **LDAP-Server** an. Die **Auswahl...** - Schaltfläche stellt eine Auswahl verfügbarer Server zur Verfügung. Auch das **Verbinden mit einer anderen Domäne** ist möglich.

Soll die Verteilung der Clients auf die einzelnen Rechner direkt im Anschluss automatisch geschehen, muss die Option **G Data Client automatisch auf neu hinzugefügten Rechnern installieren** aktiviert werden. Diese Option bewirkt auch, dass auf jedem Rechner, der zur Active Directory-Domäne zugefügt wird, sofort der Client installiert wird, sofern er die **Mindestvoraussetzungen** erfüllt. Der G Data ManagementServer gleicht seinen Datenstand regelmäßig mit dem Active Directory ab. Den Turnus, in dem der Datenstand abgefragt wird, kann individuell unter **Server-Einstellungen > Synchronisation** eingestellt werden.

Folgende Symbole sind in der Verzeichnisauswahl sichtbar:



Netzwerksymbol



Gruppe



Server (aktiviert)



Server (deaktiviert)



Client (aktiviert)



Client (deaktiviert)



Linux-Client (aktiviert)



Linux-Client (deaktiviert)



Mobile-Client (aktiviert)



Mobile-Client (deaktiviert)



Nicht auswählbare Geräte: Hierunter fallen z.B. Netzwerkdrucker

In der Symbolleiste finden Sie die wichtigsten Befehle der **Menüleiste** als anklickbare Symbole.



Ansicht aktualisieren: Über **Aktualisieren** oder die Taste **F5** können Sie die Ansicht der Administratoroberfläche jederzeit aktualisieren, um z.B. auch aktuelle Änderungen bei der Ansicht zu berücksichtigen.



Alles erweitern/reduzieren: Hiermit können Sie die Ansicht Ihres Netzwerksverzeichnis beeinflussen.



Deaktivierte Clients anzeigen: Wählen Sie diese Schaltfläche, um auch die nicht aktivierten Computer anzuzeigen. Sie erkennen die deaktivierten Computer an den grau durchscheinenden Icons. Computer ohne Dateifreigabe bzw. Druckerfreigabe werden normalerweise nicht angezeigt.



Neue Gruppe: Die aktivierten Computer können zu **Gruppen** zusammengefasst werden. Damit lassen sich leicht unterschiedliche Sicherheitszonen definieren, da alle Einstellungen sowohl für einzelne Clients als auch für komplette Gruppen durchgeführt werden können. Zum Anlegen einer neuen Gruppe markieren Sie zunächst die übergeordnete Gruppe und klicken dann auf das abgebildete Symbol.



Löschen: Sie können einen Computer aus der Liste entfernen, indem Sie ihn markieren und dann die Schaltfläche **Löschen** anklicken. Beachten Sie, dass das Löschen eines Computers aus der Clientliste nicht dazu führt, dass die Client-Software deinstalliert wird.



Client aktivieren: Zum Aktivieren eines Computers, markieren Sie ihn in der Liste und wählen dann die abgebildete Schaltfläche.

5.3 Aufgabenbereiche

In den verschiedenen Aufgabenbereichen, die über die jeweiligen Karteireiter anwählbar sind, besteht die Möglichkeit, die Absicherung der Clients zu administrieren. Die Einstellungen, die dabei vorgenommen werden, beziehen sich immer auf die Clients oder Gruppen, die im **Clientauswahlbereich** markiert wurden. Die einzelnen Themenfelder werden in den folgenden Abschnitten eingehend erläutert.

Dashboard

Im Dashboard-Bereich der G Data Software erhalten Sie Informationen zum aktuellen Zustand der Clients im Netzwerk. Diese finden sich rechts vom jeweiligen Eintrag als Text-, Zahl- oder Datumsangabe.

G Data Client Status

Hier können Sie alle grundlegenden Sicherheitseinstellungen für die Clients oder Gruppen einstellen, die Sie im Clientauswahlbereich markiert haben.



Solange das Netzwerk optimal für den Schutz vor Computerviren konfiguriert ist, finden Sie links vor den hier aufgeführten Einträgen ein grünes Symbol.



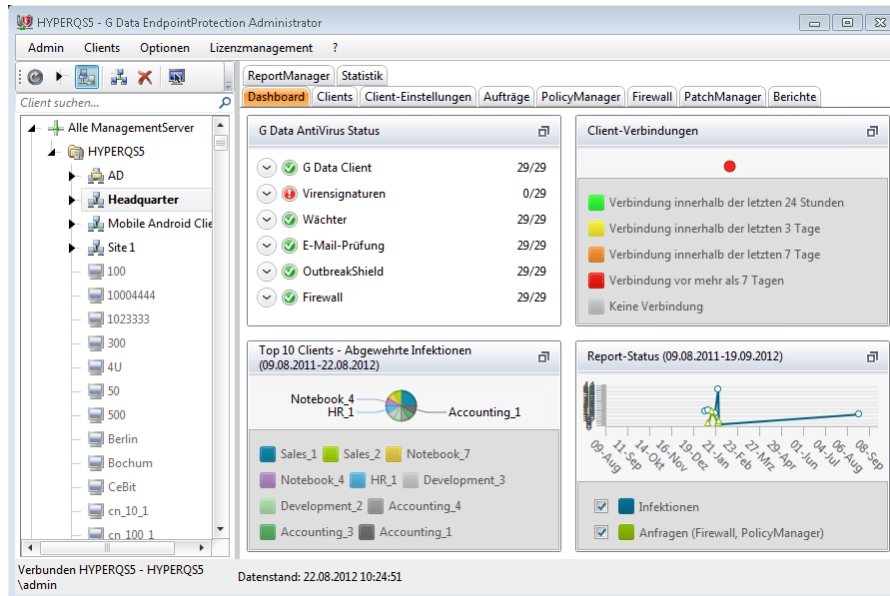
Sollte mindestens eine Komponente nicht optimal eingestellt sein (z.B. abgeschalteter Wächter oder veraltete Virensignaturen), weist ein Achtung-Symbol darauf hin.



Wenn sich die G Data-Programmoberfläche öffnet, sind in einigen Fällen für kurze Zeit die meisten Symbole im Info-Modus. Das heißt nicht, dass das Netzwerk in diesem Moment ungeschützt ist.

Hier handelt es sich um eine interne Überprüfung des Virenschutz-Status. In diesem Moment wird die Datenbank des G Data ManagementServers vom G Data Administrator abgefragt.

Durch Anklicken des jeweiligen Eintrags können Sie hier direkt Aktionen vornehmen oder in den jeweiligen Aufgabenbereich wechseln. Sobald Sie die Einstellungen einer Komponente mit Achtung-Symbol optimiert haben, wechselt das Symbol im Status-Bereich wieder auf das grüne Symbol.



Client-Verbindungen

Hier erhalten Sie eine zeitliche Übersicht über die Verbindungen, die die jeweiligen Clients oder Gruppen mit dem G Data ManagementServer hatten. Es sollte darauf geachtet werden, dass sich alle Clients regelmäßig mit dem G Data ManagementServer verbinden.

Top 10 infizierte Clients

Die Clients die z.B. aufgrund des Nutzerverhaltens oder technischer Umstände in dieser Liste erscheinen, sollten besonders beobachtet werden. Ein Auftauchen eines oder mehrerer Clients in diesem Bereich ist unter Umständen eine Indikation dafür, dass der Client-Anwender auf eventuelle Probleme aufmerksam gemacht werden oder technische Maßnahmen ergriffen werden sollten. Wenn die Infektionen auf Grund des Nutzerverhaltens stattfinden, wäre z.B. eine Nutzung des **PolicyManagers** (verfügbar in der Programmversion **G Data EndpointProtection**) ratsam.

Report-Status

Hier erhalten Sie eine übersichtliche Darstellung über die Menge der Infektionen, Anfragen und Fehler in Ihrem Netzwerk innerhalb der letzten 30 Tage.

Clients

Wählen Sie im **Clientauswahlbereich** eine Gruppe, um eine Übersicht über alle Clients der Gruppe zu erhalten. Für jeden Client wird angezeigt, welche Version der installierte Client hat, welche Version die Virensignaturen haben und wann der Client sich zum letzten Mal beim G Data ManagementServer gemeldet hat. Hier lässt sich überprüfen, ob die Clients ordnungsgemäß laufen und ob die Virensignaturen auf dem neuesten Stand sind.

Im Aufgabenbereich **Clients** stehen Ihnen alle relevanten Informationen zum Client in einer Liste zur Verfügung. Sie lassen sich durch einfaches Klicken auf die jeweilige Spaltenbezeichnung nach diversen Kriterien sortieren. Die Spalte, nach der die aktuelle Sortierung erfolgt, wird dabei durch ein kleines Pfeilsymbol gekennzeichnet.

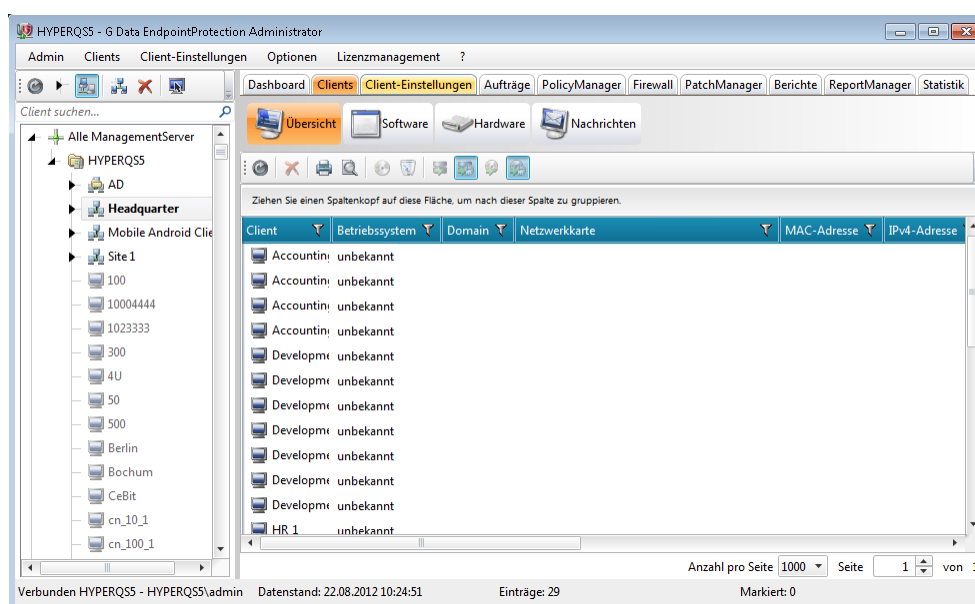
Über die oben befindlichen Schaltflächen können Sie entscheiden, ob Sie eine allgemeine **Übersicht** über die Clients bearbeiten möchten oder ob Sie den einzelnen Clients **Nachrichten** senden möchten. Mit dem Versand dieser Nachrichten können Sie Anwender schnell und unkompliziert über Änderungen am Status des Clients informieren.

Mobile Devices

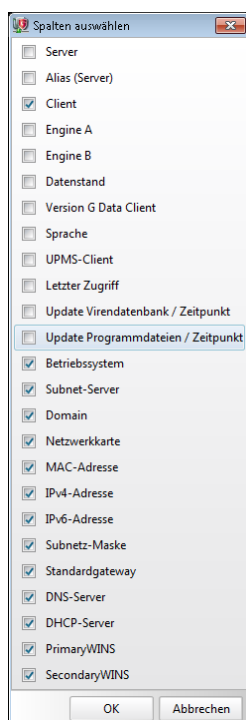
Für Clients auf Smartphones und anderen mobilen Devices gibt es einen speziellen auf diese Geräte zugeschnittenen Aufgabenbereich, der im Kapitel **Mobile Clients** erläutert wird.

Übersicht

Hier erhalten Sie eine Übersicht über alle verwalteten Clients und können diese gleichzeitig auch administrieren.



Mit einem rechten Mausklicke auf die Spaltenüberschriften können Sie weitergehende Informationsspalten zum Client zu- oder abwählen.



Zur Administration der Clients und Gruppen stehen Ihnen folgende Schaltflächen zur Verfügung.



Aktualisieren: Diese Funktion aktualisiert die Ansicht und lädt die aktuellen Clienteinstellungen vom G Data ManagementServer.



Löschen: Hiermit entfernen Sie einen Client aus der **Clientübersicht**.



Drucken: Hiermit starten Sie den Druckvorgang für die Client-Übersicht. Sie können in dem erscheinenden Auswahlfenster bestimmen, welche Details und Bereiche der Clients Sie ausdrucken möchten.



Seitenansicht: Hier können Sie vor dem eigentlichen Ausdruck eine Vorschau der zu druckenden Seiten am Monitor ausgeben.



G Data Client installieren: Diese Funktion wird im gleichnamigen Kapitel erläutert.



G Data Client deinstallieren: Diese Funktion wird im gleichnamigen Kapitel erläutert.



Virendatenbank aktualisieren: Aktualisiert die Virendatenbank auf dem Client mit den Dateien vom G Data ManagementServer.



Virendatenbank automatisch aktualisieren: Aktiviert die **automatische Aktualisierung der Virendatenbank**. Die Clients prüfen periodisch, ob aktualisierte Virensignaturen auf dem G Data ManagementServer vorhanden sind und führen die Aktualisierung automatisch durch.



Programmdateien aktualisieren: Aktualisiert die Programmdateien auf dem Client. Es werden die Client-Programmdateien verwendet, die der G Data ManagementServer bereit hält. Nach der Aktualisierung der Programmdateien kann es sein, dass der Client neu gestartet werden muss.



Programmdateien automatisch aktualisieren: Aktiviert die automatische Aktualisierung der Programmdateien. Die Clients prüfen periodisch, ob eine neue Version auf dem G Data ManagementServer existiert und führen die Aktualisierung automatisch durch.

G Data Client installieren

- 1** Damit die Clients den Server erreichen können, muss auf dem Server der **Port 7161 (TCP)** erreichbar sein.
- 2** Um die Kommunikation vom Server zum Client zu gewährleisten, muss auf dem Client **Port 7167 (TCP)** freigegeben sein.
- 3** Sofern eine Firewall verwendet wird, muss für die Datei **gdmms.exe** in dieser eine **Ausnahme** definiert sein.
- 4** In einer Windows-Arbeitsgruppe muss unter Windows XP die **einfache Dateifreigabe**, unter Windows Vista bzw. Windows 7 die Option **Freigabeassistent verwenden** deaktiviert werden. Zusätzlich sollte die Benutzerkontensteuerung (UAC) deaktiviert sein.
- 5** Ein Zugriff auf die Freigaben C\$ und Admin\$ des Clients ist erforderlich.
- 6** Es muss ein **Passwort** vergeben sein. Ein leeres Passwort ist nicht zulässig.

7

In den **Diensten** muss der **Remoteregistrierungsdienst** aktiv sein.

Der Aufruf dieser Funktion öffnet ein Dialogfenster, in dem die Zugriffsdaten für den Server eingegeben werden, über den die Installation der G Data Clients erfolgen soll. Nach Eingabe der entsprechenden Daten (die vom Programm gespeichert werden und deshalb nicht jedes mal eingegeben werden müssen), bestätigen Sie mit **OK**. Nun öffnet sich eine Dialogbox, in der sämtliche verfügbare Clients angezeigt werden. Wählen Sie hier einen oder mehrere deaktivierte Clients aus und klicken dann auf **Installieren**. Die G Data Software installiert dann automatisch die Client-Software auf den entsprechenden Rechnern. Sollte die Installation der Software über die hier beschriebene **Remote-Installation** nicht möglich sein, können Sie diese auch manuell oder mit Hilfe des **Clientinstallationspaketes** auf den Clients installieren.

Um auf **deaktivierte Clients** zugreifen zu können, müssen diese in der Clientübersicht als aktiv angezeigt werden. Bei Verwendung der Funktion **G Data Client installieren** weist Sie das Programm gegebenenfalls darauf hin und ermöglicht eine Darstellung der deaktivierten Clients.

Sie können auch eine spezielle Client-Software für **Linux-Client** installieren. Lesen Sie hierzu das Kapitel **Installation der Client-Software auf Linux-Rechnern** im Anhang dieser Dokumentation.

Nach erfolgter Clientinstallation ist ein Neustart des Clientrechners erforderlich.

Falls Sie eine Softwareversion mit einer Firewall verwenden: Bei der Installation der Client-Software werden Sie gefragt, ob auf dem Client-Rechner auch die **G Data Firewall** mitinstalliert werden soll. Weitere Informationen zur **Firewall** erhalten Sie im gleichnamigen Kapitel dieser Dokumentation.

G Data Client deinstallieren

Diese Funktion erteilt dem G Data Client den Auftrag, sich selbst zu deinstallieren. Zum vollständigen Entfernen muss der Client neu gestartet werden. Der Anwender wird durch eine Meldung dazu aufgefordert.

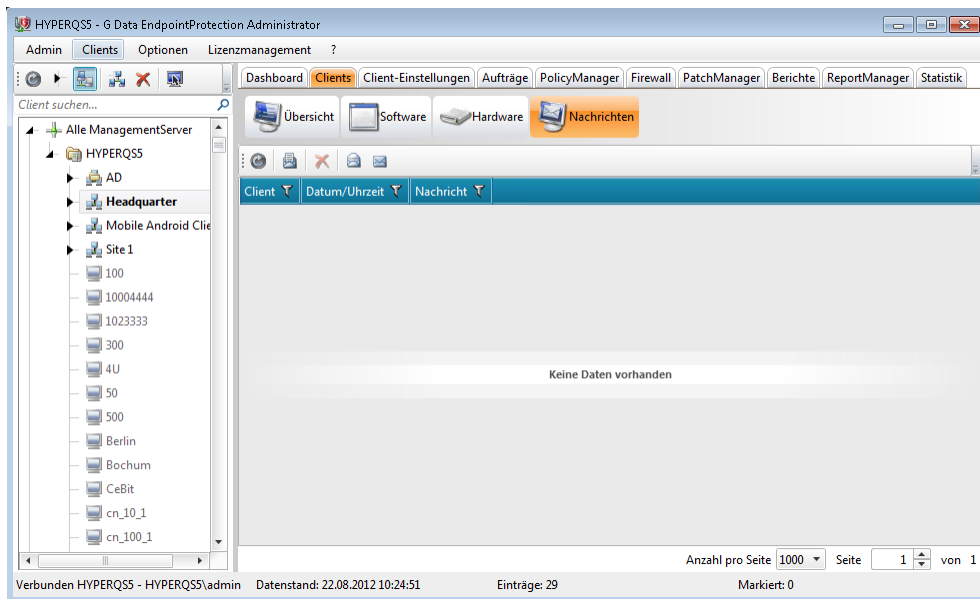
Alternativ ist es auch möglich, den Client lokal per Kommandozeilenbefehl zu deinstallieren. Hierzu ist eine Eingabeaufforderung mit Administratorberechtigungen erforderlich. Wird im Verzeichnis **C:\Programme (x86)\G DATA\AVKClient** der Befehl

UnClient /AVKUninst

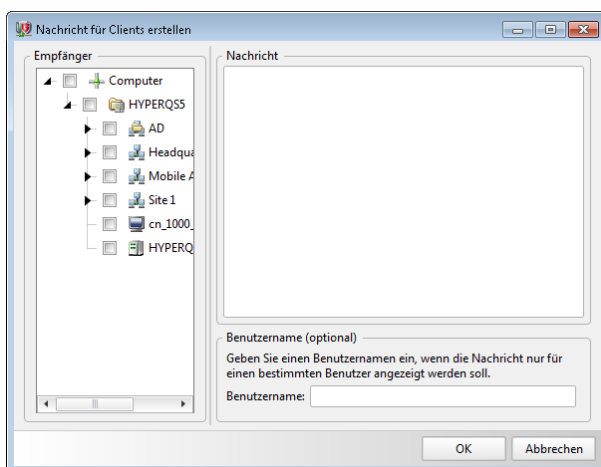
abgesetzt, startet die Deinstallation. Gegebenenfalls wird ein Neustart verlangt. Sollte eine solche Anfrage nicht erscheinen, muss der Rechner nach max. 10 Minuten neu gestartet werden.

Nachrichten

Sie als Netzwerkadministrator können an einzelne Clients oder Client-Gruppen **Nachrichten** versenden. Mit dem Versand dieser Nachrichten können Sie Anwender schnell und unkompliziert über Änderungen am Status des Clients informieren. Die Nachrichten werden dabei als Info unten rechts auf dem Desktop des Client-Rechners angezeigt.



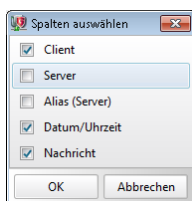
Um eine neue Nachricht zu erzeugen, klicken Sie einfach mit der rechten Maustaste in die Spaltenansicht und wählen **Neue Nachricht**. In dem nun erscheinenden Kontext-Dialog können Sie die Clients, denen Sie die Nachricht senden möchten, per Häkchen zu- oder abwählen.



Tippen Sie nun in dem Feld **Nachricht** Ihre Hinweise für die Clients ein und drücken Sie dann auf die Schaltfläche **Senden**.

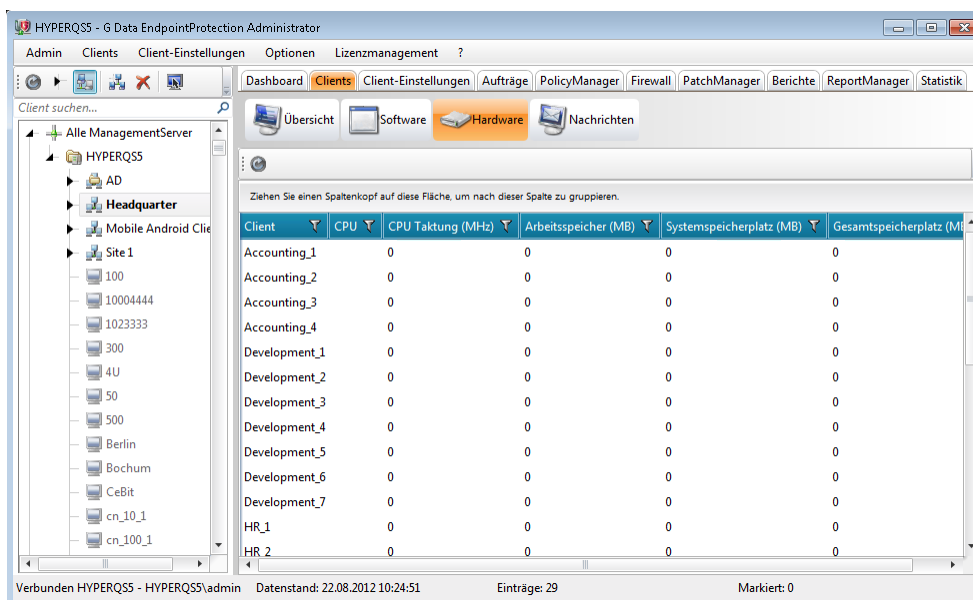
Wenn Sie eine Nachricht nur bestimmten Benutzern eines Client-Rechners oder Netzwerks zugänglich machen möchten, geben Sie dessen Anmeldenamen unter **Benutzername** ein.

Mit einem rechten Mausklick auf die Spaltenüberschriften können Sie weitergehende Informationsspalten zu den Nachrichten zu- oder abwählen.

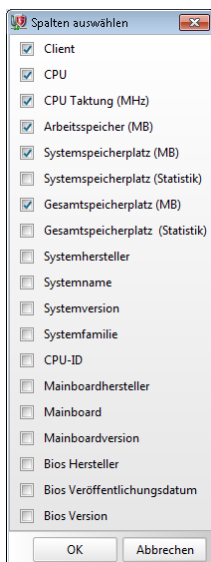


Hardware Inventar

Über diese Ansicht erhalten Sie Informationen zu der von den Clients verwendeten Hardware.

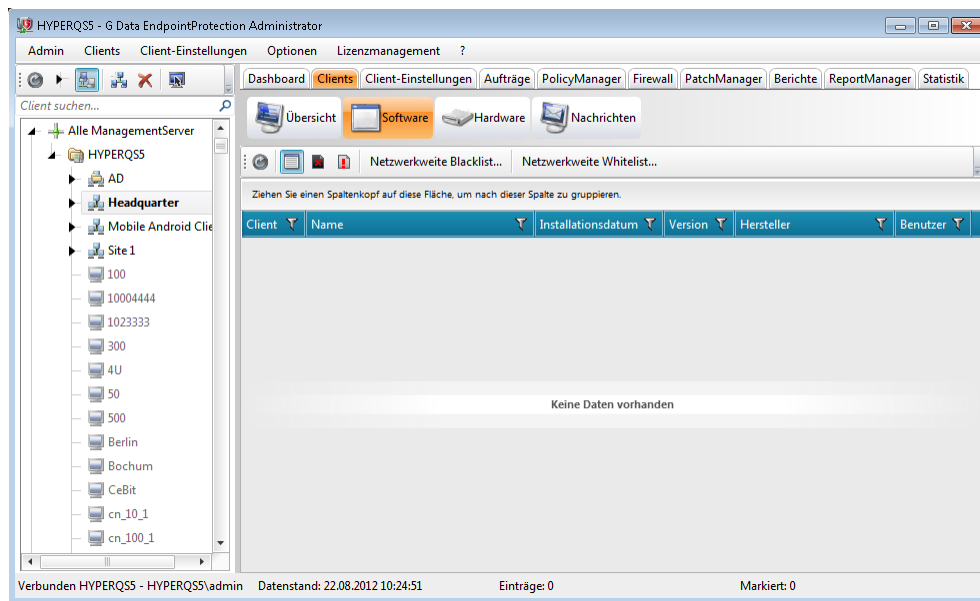


Mit einem rechten Mausklicke auf die Spaltenüberschriften können Sie weitergehende Informationsspalten zur Software zu- oder abwählen.



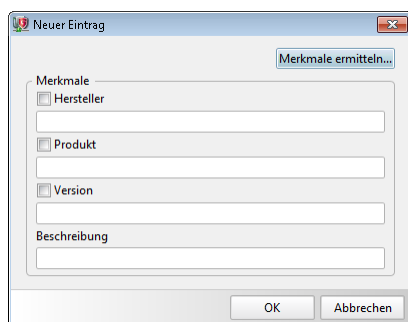
Software Inventar

Hier haben Sie die Möglichkeit, netzwerkweit die Verwendung von Software zu überwachen bzw. unternehmensweite Black-/Whitelists zu definieren.



Um die Whitelist bzw. Blacklist zu füllen, klicken Sie bitte auf die Schaltfläche **"Netzwerkweite Blacklist"** bzw. **"Netzwerkweite Whitelist"** und in dem nun erscheinenden Fenster auf die Schaltfläche **"Hinzufügen"**. Nun können Sie über die Schaltfläche **Merkmale ermitteln** im Dateibrowser die Programmdatei auswählen, die Sie blockieren bzw. erlauben möchten und die Merkmale übernehmen. Um diese ermittelten Merkmale als Auswahlkriterium zuzulassen, setzen Sie bitte das Häkchen beim jeweiligen Merkmal. So können Sie z.B. Software nur von bestimmten Herstellern erlauben oder konkrete Programmversionen einer Software zur Nutzung im Netzwerk unterbinden.

Wenn Ihnen die erforderlichen Daten zur Verfügung stehen, können Sie Software auch durch Direkteingabe der Merkmale (ohne Umweg über **Merkmale ermitteln**) auf die Black- oder Whitelist setzen.



Die Übersicht über die Elemente auf Ihrer Black-/Whitelist können Sie mit folgenden Schaltflächen beeinflussen.



Aktualisieren: Diese Funktion aktualisiert die Ansicht und lädt die aktuellen Clienteneinstellungen vom G Data ManagementServer.



Alle anzeigen: Hiermit wird Ihnen sämtliche im Netzwerk auf den Clients installierte Software angezeigt.

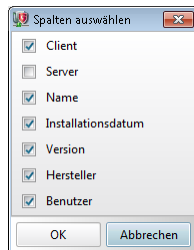


Nur Software auf der Blacklist anzeigen: Über diese Einstellung können Sie sich die Software anzeigen, die durch Ihren Eintrag auf der Blacklist auf den Clients nicht ausgeführt werden kann.



Nur Software anzeigen, die nicht auf der Whitelist ist: Hiermit erhalten Sie einen Überblick über installierte Software auf den Netzwerk-Clients, die vom Netzwerkadministrator noch nicht überprüft und kategorisiert wurde. Mit Hilfe dieser Ansicht können Sie gefundene Software mit einem Rechtsklick auf die Whitelist oder Blacklist setzen.

Mit einem rechten Mausklicke auf die Spaltenüberschriften können Sie weitergehende Informationsspalten zur Software zu- oder abwählen.



Client-Einstellungen

Allgemein

G Data Client

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Kommentar:** Geben Sie hier einen aussagekräftigen Namen für den jeweiligen Client an
- **Symbol in der Startleiste:** Für Terminal-Server und Windows mit schneller Benutzerumschaltung kann gewählt werden, in welchen Sessions ein Client-Symbol in der Taskleiste angezeigt werden soll: **nie**, **nur in der ersten Session** oder **immer**. Bei normalen Clients kann mit der Option das Anzeigen des Client-Symbols wahlweise unterbunden werden. Damit der Anwender Zugriff auf erweiterte Client-Funktionen hat, muss das Symbol angezeigt werden.
- **Benutzerkonto:** Die Client-Software läuft normalerweise im Systemkontext. Sie können hier ein anderes Konto angeben, um die Prüfung von Netzwerkverzeichnissen zu ermöglichen. Das Konto muss dazu Administratorrechte auf dem Client haben.

Updates

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Virensignaturen automatisch aktualisieren:** Aktiviert die automatische Aktualisierung der Virendatenbank. Die Clients prüfen periodisch, ob eine aktuelle Virensignaturen auf dem ManagementServer vorhanden sind. Liegen aktualisierte Virensignaturen vor, werden diese auf dem Client automatisch installiert.
- **Programmdateien automatisch aktualisieren:** Aktualisiert die Programmdateien auf dem Client. Hierzu werden die Client-Programmdateien genutzt, die der ManagementServer bereithält. Nach der Aktualisierung der Programmdateien kann es sein, dass der Client neu gestartet werden muss. Je nach Einstellung unter **Neustart nach der Aktualisierung** hat der Anwender auf dem Client die Möglichkeit, den Abschluss der Aktualisierung auf einen späteren Zeitpunkt zu verschieben.
- **Neustart nach der Aktualisierung:** Hier wird festgelegt, ob der Client nach einer Aktualisierung der Programmdateien automatisch neu gestartet wird (**Neustart ohne Abfrage**), ob dem Anwender die Möglichkeit geboten wird, den Neustart sofort oder später durchzuführen (**Hinweisfenster auf dem Client**) oder ob die Aktualisierung der Programmdateien erst dann abgeschlossen wird, wenn der Client vom Benutzer neu gestartet wird (**Bericht erzeugen**).

Client-Funktionen

Im Folgenden werden die Berechtigungen vergeben, die der Benutzer lokal für einzelne Clientfunktionen hat. So können dem Anwender umfangreiche oder auch nur stark eingeschränkte Rechte zur Änderung von Einstellungen eingeräumt werden

- **Der Anwender darf selbst Virenprüfungen durchführen:** Im akuten Verdachtsfall kann der Anwender wie bei einer lokal installierten Antivirenlösung auf seinem Rechner unabhängig vom ManagementServer eine **Virenprüfung** durchführen. Ergebnisse dieser Virenprüfung werden beim nächsten Kontakt mit dem ManagementServer an diesen übermittelt.
- **Der Anwender darf selbst Signaturupdates laden:** Wenn Sie diese Funktion aktivieren, darf der Nutzer des Clientrechners aus dem Kontextmenü heraus Virensignaturen auch ohne Verbindung zum ManagementServer direkt aus dem Internet laden.
- **Der Anwender darf die E-Mail- und Wächteroptionen ändern:** Bei Aktivierung dieser Funktion hat der Client-Anwender gezielt die Möglichkeit, neben den **Wächteroptionen** auch die Einstellungen zum Thema **E-Mail-Sicherheit** für seinen Client zu beeinflussen.
- **Lokale Quarantäne anzeigen:** Wenn das Anzeigen der lokalen **Quarantäne** erlaubt wird, kann der Anwender Daten, die vom Wächter wegen Virenbefall oder -verdacht in Quarantäne geschoben wurden ggf. desinfizieren, löschen oder zurückbewegen. Beachten Sie dabei, dass bei einem Zurückbewegen einer Datei aus der Quarantäne ein Virus nicht entfernt wird. Diese Option sollte deshalb nur versierten Anwendern auf den Clients zugänglich gemacht werden.
- **Passwortschutz für die Änderung von Optionen:** Um einer missbräuchlichen Manipulation von lokalen Einstellungen vorzubeugen, gibt es die Möglichkeit, die Änderung von Optionen nur dann zuzulassen, wenn ein Passwort eingegeben wird. So lässt sich beispielsweise verhindern, dass ein User, der normalerweise nicht am betroffenen Client arbeitet, die Einstellungen ändert. Das Passwort kann individuell für den jeweiligen Client oder die jeweilige Gruppe vergeben werden; darauf muss nur den autorisierten Nutzern dieses Passwort mitgeteilt werden.
- **Update-Einstellungen:** Hier wird festgelegt, woher die Clients ihre Virensignaturupdates beziehen. Es besteht die Möglichkeit, alle Clients unterschiedslos vom ManagementServer die Virensignaturen laden zu lassen; alternativ kann das Recht eingeräumt werden, selbst die Aktualisierungen durchzuführen. Für mobile Arbeitsplätze empfiehlt sich ein Mischbetrieb, d.h. solange der Client eine Verbindung zum ManagementServer hat, bezieht er die Aktualisierungen von dort. Besteht keine Verbindung zum ManagementServer mehr, werden die Virensignaturen automatisch aus dem Internet geladen. Über die Schaltfläche **Einstellungen und Zeitplanung** können des Weiteren für den jeweiligen Client Einstellungen vorgenommen werden, je nach Einsatzumgebung erforderlich sind, um den Download der Virensignaturen zu ermöglichen. Auch die Intervalle, in denen Aktualisierungen vorgenommen werden, können hier definiert werden.

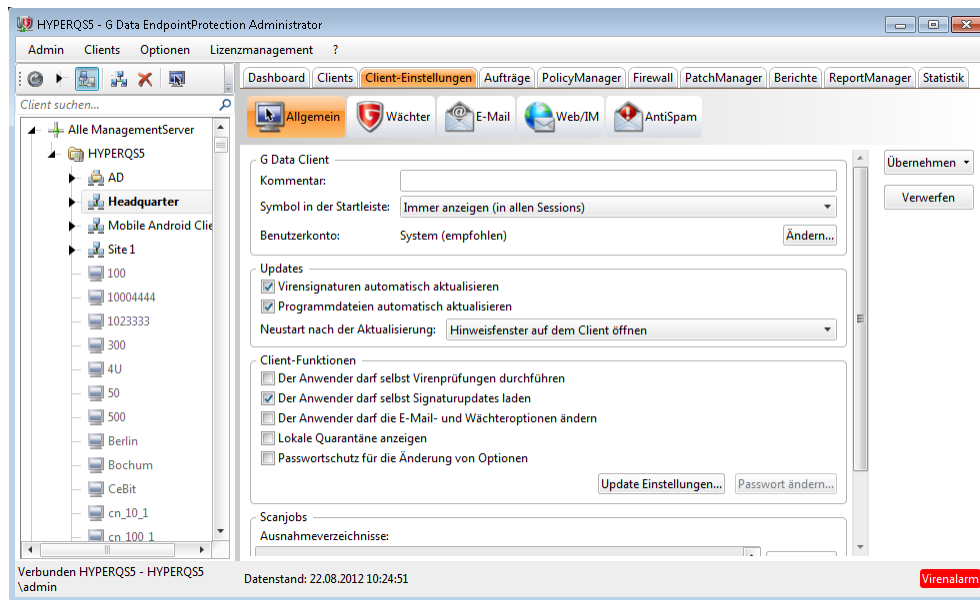
Ausnahmeverzeichnisse für Scanaufträge

Hier werden Ausnahmeverzeichnisse auf den Clients definiert, die bei der Durchführung von Scanaufträgen nicht geprüft werden sollen. Beispielsweise können Archiv- und Backup-Bereiche einer Festplatte oder Partition als Ausnahmeverzeichnisse definiert werden.

Ausnahmeverzeichnisse können für komplette **Gruppen** definiert werden. Falls die Clients in einer Gruppe unterschiedliche Ausnahmeverzeichnisse definiert haben, können neue Verzeichnisse hinzugefügt oder vorhandene gelöscht werden. Die speziell für einzelne Clients definierten Verzeichnisse bleiben dabei erhalten. Das gleiche Verfahren wird auch bei den Wächterausnahmen angewendet.

Besonderheit auf einem Linux-Fileserver

Bei der Auswahl von Ausnahmeverzeichnissen werden das Root-Laufwerk (/) und alle Freigaben zurück geliefert. Dabei können Laufwerks-, Verzeichnis- und Dateiausnahmen angelegt werden.



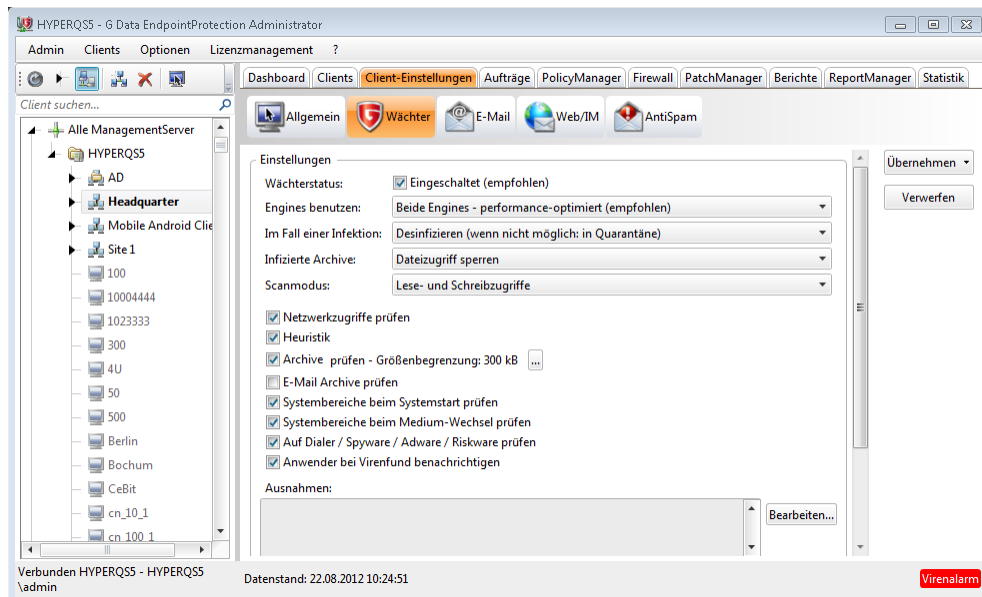
Wächter

Hier können die Wächtereinstellungen für den im **Clientauswahlbereich** gewählten Client bzw. die ausgewählte Gruppe vorgenommen werden. Die geänderten Einstellungen werden erst nach Betätigung der **Übernehmen**-Schaltfläche gespeichert. Drücken Sie die **Verwerfen**-Schaltfläche, um die aktuellen Einstellungen vom ManagementServer zu laden, ohne die Änderungen zu übernehmen.

Sollten Client innerhalb einer Gruppe unterschiedliche Einstellungen haben, wird bei Parametern, die unterschiedlich eingestellt sind einzelne Parameter einen undefinierten Status einnehmen. Die Clients der Gruppe haben in diesem Fall unterschiedliche Einstellungen für die Parameter. Undefinierte Parameter werden beim Übernehmen nicht gespeichert.

Der Wächter sollte grundsätzlich nicht deaktiviert werden, da dieser für den Echtzeitschutz vor Schädlingen sorgt. Wird der Wächter deaktiviert, besteht dieser Schutz nicht mehr. Es wird daher empfohlen, den Wächter nur dann auszuschalten, wenn ein berechtigtes Interesse daran besteht, zum Beispiel Fehlersuche oder Diagnose.

Die Definition von Ausnahmen für den Wächter ist möglich. Sollte eine Anwendung durch den Einsatz des Wächters mit Performanceeinbußen zu kämpfen haben, können für die entsprechenden Programmdateien, Prozesse oder Dateien Ausnahmen hinzugefügt werden; ausgenommene Dateien werden dann nicht mehr vom Wächter geprüft. Beachten Sie, dass das Hinzufügen von Wächterausnahmen unter Umständen ein Sicherheitsrisiko darstellen kann.



Einstellungen

Folgende Funktionen stehen Ihnen im Einstellungen-Bereich zur Verfügung:

- **Wächterstatus:** Hier können Sie den Wächter anschalten bzw. ausschalten. Generell sollten Sie den Wächter eingeschaltet lassen. Er ist die Grundlage für einen permanenten und lückenlosen Virenschutz.
- **Engines benutzen:** Die G Data Software arbeitet mit zwei unabhängig voneinander operierenden Virenanalyseeinheiten. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Virenprophylaxe. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich.
- **Im Fall einer Infektion:** Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Je nachdem, für welche Zwecke der jeweilige Client verwendet wird, sind hier unterschiedliche Einstellungen sinnvoll.

Dateizugriff sperren: Auf eine infizierte Datei können weder Schreib- noch Lesezugriffe ausgeführt werden.

Desinfizieren (wenn nicht möglich: Zugriff sperren): Hier wird versucht, den Virus zu entfernen, falls das nicht möglich ist, dann wird der Dateizugriff gesperrt.

Desinfizieren (wenn nicht möglich: in Quarantäne): Hier wird versucht, den Virus zu entfernen. Falls dies nicht möglich ist, wird die Datei in die **Quarantäne** verschoben.

Desinfizieren (wenn nicht möglich: Datei löschen): Hier wird versucht, den Virus zu entfernen. Falls dies nicht möglich ist, wird die Datei gelöscht. Allerdings kann es dabei im seltenen Fall einer falsch-positiven Virenmeldung zu Datenverlust kommen.

Datei in Quarantäne verschieben: Hier wird die infizierte Datei in die Quarantäne verschoben. Eine mögliche Desinfektion der Datei kann dann manuell durch den Systemadministrator durchgeführt werden.

Infizierte Datei löschen: Als rigorose Maßnahme hilft diese Funktion dabei, den Virus wirkungsvoll einzudämmen. Allerdings kann es dabei im seltenen Fall einer falsch-positiven Virenmeldung zu Datenverlust kommen.

- **Infizierte Archive:** Legen Sie hier fest, wie infizierte **Archive** behandelt werden sollen. Beachten Sie beim Festlegen dieser Einstellungen, dass ein Virus innerhalb eines Archives erst dann Schaden anrichtet, wenn das Archiv entpackt wird.
- **Dateitypen:** Hier können Sie festlegen, welche Dateitypen von G Data auf Viren untersucht werden sollen. Beachten Sie, dass eine Überprüfung aller Dateien eines Computers eine gewisse Zeit in Anspruch nehmen kann.

- **Beim Schreiben prüfen:** Normalerweise erzeugt ein virenfrees System beim Schreiben von Dateien keine virenfürzten Dateien. Um jedoch alle Eventualitäten auszuschließen, können Sie hier für einen Scanvorgang beim Schreiben von Dateien sorgen. Der immense Vorteil liegt hier darin, dass so auch Viren erkannt werden, die von einem anderen, möglicherweise ungeschützten Client, auf ein freigegebenes Verzeichnis des durch den Wächter geschützten Clients kopiert werden und dass aus dem Internet geladene Dateien schon beim Ladevorgang und nicht erst beim Ausführen als virenbehaftet erkannt werden.
- **Netzwerkzugriffe prüfen:** Hier können Sie die Vorgehensweise des Wächters im Zusammenhang mit Netzwerkzugriffen festlegen. Wenn Sie ihr gesamtes Netzwerk generell mit der G Data Software überwachen, kann eine Überprüfung der Netzwerkzugriffe entfallen.
- **Heuristik:** In der heuristischen Analyse werden Viren nicht nur anhand der ständig aktualisierten Virendatenbanken ermittelt, sondern auch anhand bestimmter virentypischer Merkmale erkannt. Diese Methode ist einerseits ein weiteres Sicherheitsplus, andererseits kann in seltenen Fällen auch ein **Fehlalarm** erzeugt werden.
- **Archive prüfen:** Das Überprüfen gepackter Daten in Archiven ist sehr zeitintensiv und kann in der Regel dann unterbleiben, wenn der G Data Virenwächter auf dem System aktiv ist. Dieser erkennt dann beim Entpacken des Archives einen bis dahin verborgenen Virus und unterbindet automatisch dessen Verbreitung. Um die Performance durch das unnötige Überprüfung großer Archiv-Dateien, die selten verwendet werden, nicht zu belasten, können Sie die Größe der Archivdateien, die durchsucht werden, auf einen bestimmten Wert in Kilobyte begrenzen.
- **E-Mail Archive prüfen:** Diese Option sollte in der Regel ausgeschaltet werden, da die Prüfung von E-Mail-Archiven in der Regel sehr lange dauert und im Falle einer infizierten Mail eine Mailbox - abhängig von den Einstellungen des Virenschans - in die Quarantäne verschoben oder gelöscht wird. Mail Mails innerhalb des Mailarchivs wären in einem solchen Fall nicht mehr verfügbar. Da der Wächter die Ausführung von infizierten E-Mail-Anhängen blockiert, wird durch das Ausschalten dieser Option kein Sicherheitsloch geschaffen. Bei der Verwendung von **Outlook** werden die ein- und ausgehenden Mails zusätzlich durch ein integriertes PlugIn geprüft.
- **Systembereiche beim Systemstart prüfen:** Systembereiche (z.B. **Bootsektoren**) Ihres Computers sollten nicht von der Virenkontrolle ausgeschlossen werden. Sie können hier festlegen, ob Sie diese beim Systemstart überprüfen oder beim Medium-Wechsel (neue DVD o.ä.). Generell sollten Sie zumindest eine dieser beiden Funktionen aktiviert haben.
- **Systembereiche beim Medium-Wechsel prüfen:** Systembereiche (z.B. **Bootsektoren**) Ihres Computers sollten in der Regel nicht von der Virenkontrolle ausgeschlossen werden. Sie können hier festlegen, ob Sie diese beim Systemstart überprüfen oder beim **Medium-Wechsel** (neue DVD o.ä.). Generell sollten Sie zumindest eine dieser beiden Funktionen aktiviert haben.
- **Auf Dialer / Spyware / Adware / Riskware prüfen:** Mit der G Data Software können Sie Ihr System auch auf **Dialer** und andere Schadprogramme (**Spyware, Adware, Riskware**) überprüfen. Hierbei handelt es sich z.B. um Programme, die unerwünschte teure Internetverbindungen aufbauen und in ihrem wirtschaftlichen Schadpotential dem Virus in nichts nachstehen. Spyware kann z.B. Ihr Surfverhalten oder sogar sämtliche Tastatureingaben (und damit auch Ihre Passwörter) unbemerkt speichern und bei nächster Gelegenheit übers Internet an fremde Personen weiterleiten.
- **Anwender bei Virenfund benachrichtigen:** Wird diese Option aktiviert, öffnet sich bei einem Virenfund durch den Wächter auf dem betroffenen Client ein Hinweisfenster, das den Anwender darüber in Kenntnis setzt, dass auf seinem System ein Virus gefunden wurde. Die gefundene Datei sowie der Pfad und die Bezeichnung des gefundenen Schädlings werden dort angezeigt.

Ausnahmen

Hier können Sie beim Client die Virenprüfung auch auf bestimmte Verzeichnisse begrenzen. Auf diese Weise können Sie z.B. Ordner mit selten benötigten Archiven aussparen, um diese in einem gesonderten Scanauftrag zu prüfen. Des Weiteren lassen sich bestimmte Dateien und Dateitypen von der Virenprüfung ausschließen. Folgende Ausnahmen sind möglich:

- **Laufwerk:** Wählen Sie hier mit Anklicken der Verzeichnis-Schaltfläche ein Laufwerk (**Partition, Festplatte**) aus, welches Sie vom Wächter nicht kontrollieren lassen möchten.
- **Verzeichnis:** Wählen Sie hier mit dem Anklicken der Verzeichnis-Schaltfläche einen **Ordner** (gegebenenfalls inkl. seiner darin befindlichen **Unterordner**) aus, der nicht vom Wächter kontrolliert werden soll.

- **Datei:** Hier können Sie den Namen der Datei eingeben, die Sie von der Wächterkontrolle ausnehmen möchten. Sie können hier auch mit Platzhaltern arbeiten.
- **Prozess:** Soll ein bestimmter Prozess nicht vom Wächter überwacht werden, ist der Name des betreffenden Prozesses hier einzutragen.

Sie können diesen Vorgang bei Bedarf beliebig oft wiederholen und im **Wächter Ausnahmen**-Fenster vorhandene Ausnahmen auch wieder löschen oder modifizieren.

Die Funktionsweise von **Platzhaltern** ist folgendermaßen:

- Das **Fragezeichen-Symbol** (?) ist Stellvertreter für einzelne Zeichen.
- Das **Sternchen-Symbol** (*) ist Stellvertreter für ganze Zeichenfolgen.

Um z.B. sämtliche Dateien mit der Dateiendung **exe** schützen zu lassen, geben Sie also ***.exe** ein. Um z.B. Dateien unterschiedlicher Tabellenkalkulationsformate zu schützen (z.B. **xlr**, **xls**), geben Sie einfach ***.xl?** ein. Um z.B. Dateien unterschiedlichen Typs mit einem anfänglich gleichen Dateinamen zu schützen, geben Sie beispielsweise **text*.*** ein. Dies würde die Dateien *text1.txt*, *text2.txt*, *text3.txt* usw. betreffen.

Verhaltensüberwachung

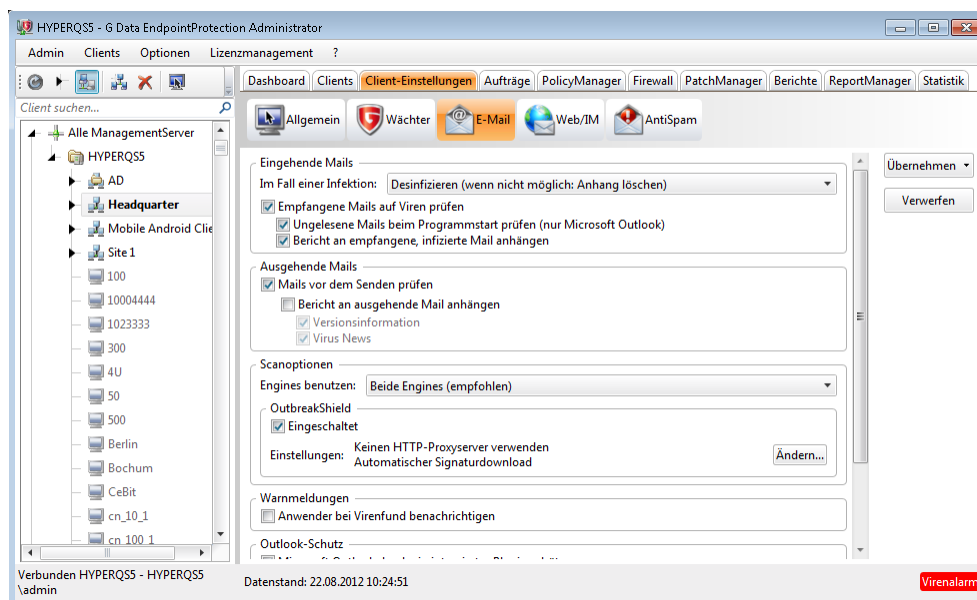
Die Verhaltensüberwachung stellt einen weiteren Schutz vor schädlichen Dateien dar, der im Unterschied zum Wächter, nicht signaturbasiert arbeitet, sondern das tatsächliche Verhalten einer Datei analysiert. Um eine Einordnung vorzunehmen, legt die Verhaltensüberwachung verschiedene Kriterien zugrunde, unter anderem Schreibzugriffe auf die Registry und das eventuelle Anlegen von Autostarteinträgen. Sind genügend Merkmale vorhanden, die den Schluss zulassen, dass ein Programm zumindest verdächtiges Verhalten an den Tag legt, wird die unter **Im Fall einer Bedrohung** eingestellte Aktion durchgeführt. Hierbei stehen die Optionen **Nur protokollieren**, **Programm anhalten** sowie **Programm anhalten und in Quarantäne verschieben** zur Verfügung. Bei der Einstellung **Nur protokollieren** wird das Programm nicht weiter beeinflusst und es wird nur unter **Berichte** eine entsprechende Meldung angezeigt.

Status

Hier wird Ihnen angezeigt, ob die am Wächter durchgeführten Änderungen schon für den Client oder die Gruppe übernommen wurden oder Sie die **Übernehmen**-Schaltfläche noch drücken müssen.

E-Mail

Auf jedem G Data Security Client kann ein gesonderter Virenschutz für E-Mails eingerichtet werden. Hierbei werden Standardports für die Protokolle **POP3**, **IMAP** und **SMTP** überwacht. Für **Microsoft Outlook** findet darüber hinaus ein spezielles **Plug-In** Verwendung. Das Plug-In überprüft automatisch alle eingehenden Mails auf Viren und verhindert, dass infizierte Mails versendet werden. Durch Betätigen der Schaltfläche **Übernehmen** akzeptieren Sie dabei durchgeführte Änderungen, mit **Verwerfen** werden alle vorgenommenen Änderungen rückgängig gemacht. Über den G Data Administrator können Sie für jeden Client oder für Benutzergruppen individuelle Konfigurationen für den Umgang mit Mails erstellen.



Eingehende Mails

Folgende Funktionen stehen hier zur Verfügung:

- **Im Fall einer Infektion:** Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Je nachdem, für welche Zwecke der jeweilige Client verwendet wird, sind hier unterschiedliche Einstellungen sinnvoll.
- **Empfangene Mails auf Viren prüfen:** Mit Aktivierung dieser Option werden sämtliche E-Mails auf Viren überprüft, die den Client online erreichen.
- **Ungelesene Mails beim Programmstart prüfen (nur für Microsoft Outlook):** Diese Option dient dazu, E-Mails auf Virenbefall zu kontrollieren, die den Client erreichen, während dieser nicht mit dem Internet verbunden ist. Sobald **Outlook** geöffnet wird, werden deshalb sämtliche ungelesene Mails im Posteingang-Ordner und den darin enthaltenen Unterordnern kontrolliert.
- **Bericht an empfangene, infizierte Mails anhängen:** Sobald eine an den Client geschickte E-Mail einen Virus enthält, erhalten Sie im Body dieser Mail unter dem eigentlichen Mailtext die Meldung **ACHTUNG! Diese Mail enthält folgenden Virus** gefolgt vom Namen des Virus. Außerdem finden Sie vor dem eigentlichen Betreff die Mitteilung **[VIRUS]**. Sollten Sie die Option **Anhang/Text löschen** aktiviert haben, wird Ihnen außerdem mitgeteilt, dass der infizierte Teil der E-Mail gelöscht wurde.

Ausgehende Mails

Folgende Funktionen stehen hier zur Verfügung:

- **Mails vor dem Senden prüfen:** Damit aus Ihrem Netzwerk keine Viren per Mail verschickt werden, bietet die G Data Software auch die Möglichkeit, Mails vor dem Versenden auf Virenbefall zu überprüfen. Sollte tatsächlich ein Virus versendet werden, erscheint die Meldung **Die Mail [Betreffzeile] enthält folgenden Virus: [Virusname]**. Die entsprechende E-Mail wird nicht versandt.
- **Bericht an ausgehende Mails anhängen:** Ein Prüfbericht wird im Body jeder ausgehenden E-Mail unter dem eigentlichen Mailtext angezeigt. Dieser lautet **Virengeprüft von G Data AntiVirus**, so lange Sie die Option **Mails vor dem Senden prüfen** aktiviert haben. Zusätzlich können Sie hier das Versionsdatum von G Data AntiVirus (**Versionsinformation**) angeben.

Scanoptionen

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Engines benutzen:** Die G Data Software arbeitet mit zwei unabhängig voneinander operierenden Virenanalyseeinheiten, den so genannten Engines. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenprophylaxe. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich; d.h. wenn Sie nur eine Engine verwenden, kann eine Analyse schneller durchgeführt werden.

- **OutbreakShield:** Mit dem OutbreakShield können Schädlinge in Massenmails schon erkannt und bekämpft werden, bevor aktualisierte Virensignaturen dafür verfügbar sind. Das OutbreakShield erfragt dabei über das Internet besondere Häufungen von verdächtigen Mails und schließt dabei in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Virensignaturen besteht. Unter **Ändern** können Sie festlegen, ob das OutbreakShield zur Steigerung der Erkennungsleistung zusätzliche Signaturen verwendet. Außerdem können Sie hier Zugangsdaten für die Internetverbindung oder einen Proxyserver eingeben, die dem OutbreakShield automatische Signaturdownloads aus dem Internet ermöglichen.

Warnmeldungen

Anwender bei Virenfund benachrichtigen: Sie können den Empfänger einer infizierten Nachricht automatisch informieren. Auf seinem Desktop wird dann eine Virenmeldung angezeigt.

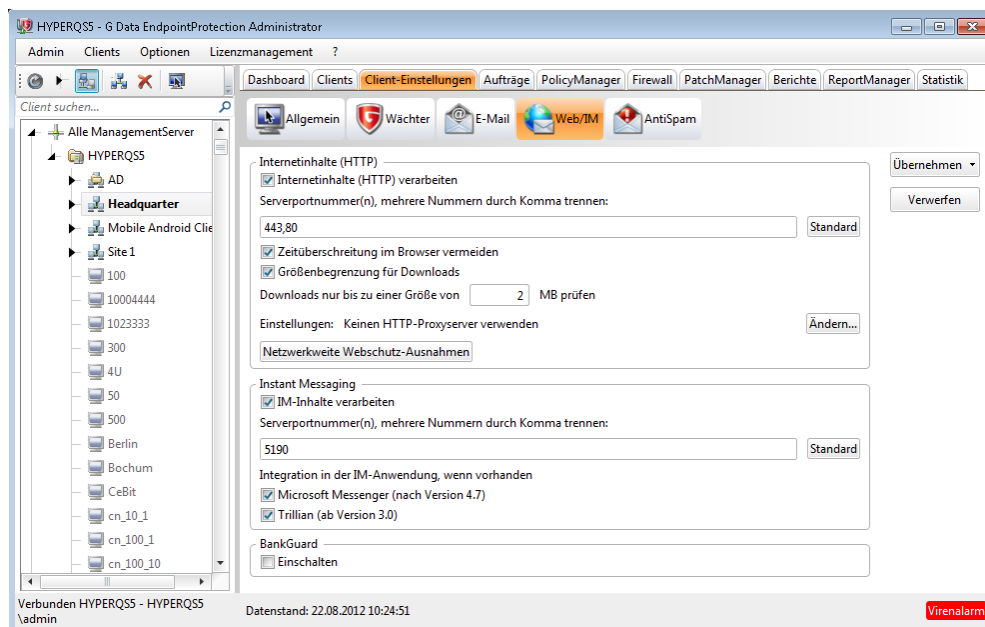
Outlook-Schutz

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Microsoft Outlook durch ein integriertes Plug-In schützen:** Mit Aktivierung dieser Funktion wird in das **Outlook** des Clients im Menü **Extras** eine neue Funktion namens **Ordner auf Viren überprüfen** eingefügt. Unabhängig von den G Data Administrator-Einstellungen kann der Nutzer des einzelnen Clients den jeweils momentan ausgewählten Mailordner nach Viren durchsuchen. Im Ansichtsfenster einer E-Mail können Sie im Menü **Extras** über **Mail auf Viren überprüfen** eine Virenprüfung der Dateianlagen durchführen. Nach Abschluss des Vorgangs erscheint ein Info-Bildschirm, in dem das Ergebnis der Virenprüfung zusammengefasst wird. Hier erfahren Sie, ob die Virenanalyse vollständig erfolgte, erhalten Infos über die Anzahl der untersuchten Mails und Dateianhänge, etwaige Lesefehler sowie über gefundene Viren und wie damit verfahren wurde. Beide Fenster können Sie mit einem Klick auf die Schaltfläche **Schließen** ausblenden.
- **Port-Überwachung:** Generell werden die **Standardports** für **POP3 (110)**, **IMAP (143)** und **SMTP (25)** überwacht. Sollten die Porteeinstellungen in Ihrem System davon abweichen, können Sie dies entsprechend anpassen.

Web/IM

Folgende Einstellungen können Sie hier vornehmen.



Internetinhalte (HTTP)

- **Internetinhalte (HTTP) verarbeiten:** In den Web-Optionen können Sie bestimmen, dass sämtliche **HTTP-Webinhalte** schon beim Browsen auf Viren überprüft werden. Infizierte Webinhalte werden dann gar nicht erst ausgeführt und die entsprechenden Seiten nicht angezeigt. Setzen Sie hierzu das Häkchen bei **Internetinhalte (HTTP) verarbeiten**.

Wird im Netzwerk ein Proxy für den Zugang zum Internet genutzt, muss der Serverport eingetragen werden, den der Proxy nutzt. Sonst ist eine Überprüfung des Internetverkehrs nicht möglich. Auch die Webinhaltskontrolle (verfügbar in der G Data EndpointProtection) benutzt diese Einstellungen.

- **Zeitüberschreitung im Browser vermeiden:** Da die G Data Software die Webinhalte vor Ihrer Darstellung im Internet Browser bearbeitet und dafür je nach Datenaufkommen eine gewisse Zeit benötigt, kann es vorkommen, dass eine Fehlermeldung im Internet Browser erscheint, weil dieser nicht sofort die angeforderten Daten erhält, da diese zunächst von der Antivirensoftware auf Schadroutinen überprüft werden. Mit Setzen des Häkchens bei **Zeitüberschreitung im Browser vermeiden** wird diese Fehlermeldung unterdrückt. Sobald sämtliche Browserdaten auf Viren überprüft wurden, werden diese dann an den Internet Browser weitergereicht.
- **Größenbegrenzung für Downloads:** Hiermit können Sie die HTTP-Überprüfung für zu große Webinhalte aussetzen. Die Inhalte werden dann vom Virenwächter überprüft, sobald etwaige Schadroutinen aktiv werden. Der Vorteil bei dieser Größenbegrenzung liegt darin, dass es beim Download größerer Dateien nicht zu Verzögerungen durch die Virenkontrolle kommt.
- **Unternehmensweite Webschutz-Ausnahmen:** Diese Funktion erlaubt es Ihnen, bestimmte Webseiten generell von der Überprüfung durch den Webschutz auszunehmen.

Instant Messaging

- **IM-Inhalte verarbeiten:** Da auch über Instant Messaging-Programme Viren und andere Schadprogramme verbreitet werden, kann die G Data Software auch hier die Anzeige und den Download infizierter Daten im Vorfeld unterbinden. Sollten die verwendeten Instant Messaging-Anwendungen nicht die Standardports nutzen, geben Sie unter **Serverportnummer(n)**, die entsprechenden Ports ein.
- **Instant Messaging (Integration in der IM-Anwendung):** Sollten Sie den **Microsoft Messenger (ab Version 4.7)** oder **Trillian (ab Version 3.0)** verwenden, steht durch Setzen des Häkchens für das jeweilige Programm ein Kontextmenü zur Verfügung, in dem Sie verdächtige Dateien direkt auf Viren überprüfen können.

Wenn Sie die Internetinhalte nicht prüfen lassen wollen, greift der **Virenwächter** ein, wenn auf heruntergeladenen, infizierten Dateien zugegriffen wird. Das System auf dem jeweiligen Client ist also auch ohne die Überprüfung von Internetinhalten geschützt, solange der Virenwächter aktiviert ist.

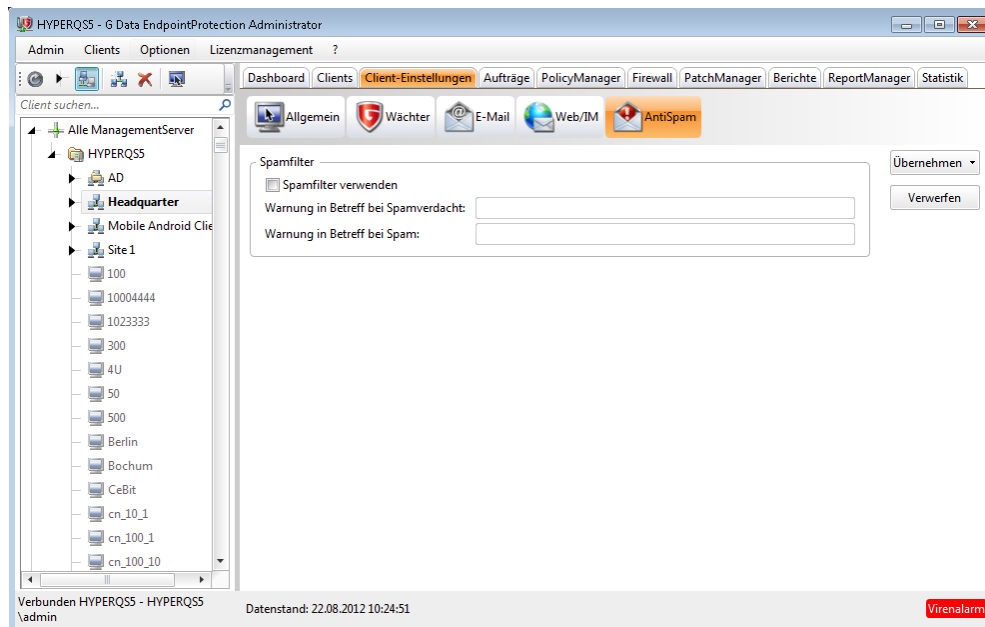
BankGuard

Banking-Trojaner werden zu einer immer größeren Bedrohung. Die wegweisende Technologie von G Data BankGuard sichert Bankgeschäfte von Anfang an und schützt sofort dort, wo der Angriff stattfindet. Durch eine Prüfung der Echtheit der benutzten Netzwerkbibliotheken stellt G Data BankGuard sicher, dass Internet-Browser nicht von einem Banking-Trojaner manipuliert werden. Durch diesen proaktiven Sofortschutz von mehr als 99 % sind Online-Bankgeschäfte bestmöglich geschützt - selbst vor bisher unbekannten Trojanern. Sollten Bankgeschäfte über Clients in Ihrem System geführt werden, sollten Sie diesen zusätzlichen Schutz für Ihre Clients aktivieren.

AntiSpam

Wenn Sie das Häkchen bei **Spamfilter verwenden** setzen, wird der E-Mail-Verkehr des Clients auf eventuelle Spam-Mails überprüft. Sobald eine E-Mail als Spam erkannt wird oder unter Spamverdacht fällt, können Sie eine Warnung festlegen, die dann im Betreff der Mail angezeigt wird.

Über die Warnung können Sie - oder der Anwender - auf dem Client im Mailprogramm eine Regel definieren, nach der z.B. Mails, die die Meldung **[Spam]** in der Betreffzeile haben, automatisch in einen speziellen Ordner für Spam- und Junk-Mail verschoben werden.



Aufträge

In diesem Aufgabenbereich werden Aufträge für Virenprüfungen auf den G Data Clients definiert. Es gibt zwei unterschiedliche Auftragsarten: **Einmalige Scanaufträge** und **periodische Scanaufträge**. Die einmaligen Jobs werden einmal zum festgelegten Zeitpunkt ausgeführt, für die periodischen wird ein **Zeitplan** definiert, nach dem sie ausgeführt werden sollen.

Als **Scanaufträge** bzw. **Jobs** werden alle Aufträge bezeichnet, die am G Data ManagementServer erstellt werden. Es kann sich hier um Scanaufträge, Backup- oder Wiederherstellungsaufträge handeln.

Im Aufgabenbereich **Aufträge** erscheinen alle Jobs unter den von Ihnen vorgegebenen Namen und lassen sich durch einfaches Klicken auf die jeweilige Spaltenbezeichnung nach folgenden Kriterien sortieren. Die Spalte, nach der die aktuelle Sortierung erfolgt, wird dabei durch ein kleines Pfeilsymbol gekennzeichnet:

- **Name:** Der von Ihnen vorgegebene Name für den Job. Sie können hier beliebig lange Namen eingeben und auf diese Weise Ihren Job genau beschreiben, um bei vielen verschiedenen Jobs den Überblick zu behalten.
- **Client:** Hier finden Sie den Namen des jeweiligen Clients. Sie können Jobs nur für aktivierte Clients definieren.
- **Gruppe:** Sie können einzelne Clients zu Gruppen zusammenfassen, die dann dieselben Jobs nutzen. Wenn Sie einer Gruppe einen Job zuordnen, erscheinen in der Übersichtsliste nicht die einzelnen Rechner, sondern der Gruppenname.
- **Status:** Hier erhalten Sie den Status oder das Ergebnis eines Jobs im Klartext angezeigt. So erfahren Sie z.B., ob der Job gerade durchgeführt oder abgeschlossen wurde und werden auch darüber informiert, ob Viren gefunden wurden oder nicht.
- **Letzte Ausführung:** Über diese Spalte erhalten Sie Informationen darüber, wann der jeweilige Job das letzte Mal durchgeführt wurde.
- **Zeitintervall:** Gemäß der **Zeitplanung**, die Sie für jeden Job definieren können, steht hier, in welchem Turnus der Job wiederholt wird.
- **Umfang:** Hier erfahren Sie auf welche **Datenträger** (z.B. lokale Festplatten) sich die Analyse erstreckt.

In der Menüleiste steht Ihnen für den Aufgabenbereich **Aufträge** ein zusätzlicher Menüeintrag mit folgenden Funktionen zur Verfügung:

- **Ansicht:** Wählen Sie hier aus, ob Sie sich alle Aufträge, oder nur ausgewählte Jobs (z.B. Softwareerkennungsaufträge, Backupaufträge, Scan-Aufträge) anzeigen lassen möchten. Für Scanaufträge, die für eine **Gruppe** von Clients definiert wurden, können Sie festlegen, ob detaillierte Infos zu allen Clients oder nur gruppenübergreifende Zusammenfassungen angezeigt werden sollen. Setzen Sie hierzu das Häkchen bei **Gruppenjobs ausführlich anzeigen**.
- **Sofort (erneut) ausführen:** Hiermit können Sie ausgewählte Jobs unabhängig von eingestellten zeitlichen Vorgaben direkt ausführen.
- **Abbrechen:** Über diese Funktion können Sie einen laufenden Job abbrechen.
- **Löschen:** Ausgewählte Jobs können mit dieser Funktion gelöscht werden.
- **Backup wiederherstellen:** Hiermit können Sie übers Netzwerk Backups auf den Clients einspielen.
- **Neu:** Wählen Sie hier aus, ob Sie einen **einmaligen Scanauftrag** (einmaliges Prüfen) oder einen **regelmäßigen Scanauftrag** (periodisches Prüfen) erstellen wollen. Sie können außerdem einen Backup- bzw. Wiederherstellungjob erstellen.*

Sie können beliebig viele unterschiedliche Scanaufträge definieren. Generell ist es aus Gründen der Performance allerdings sinnvoll, dass sich Scanaufträge zeitlich nicht überschneiden.

* Dies ist von Ihrer Produktversion abhängig.

Einstellungs- und Ansichtsoptionen



Aktualisieren: Diese Funktion aktualisiert die Ansicht und lädt die aktuelle Jobliste vom G Data ManagementServer.



Löschen: Die Funktion **Löschen...** löscht alle markierten Jobs.



Einmaliger Scanauftrag: Mit dieser Funktion lassen sich Scanaufträge für einzelne Rechner oder Rechnergruppen definieren. Im Konfigurationsdialog lassen sich auf den jeweiligen Karteireitern Analyseumfang und weitere Scaneinstellungen festlegen. Erfahren Sie mehr zu den Einstellungsmöglichkeiten für Scanaufträge im Kapitel **Scanaufträge definieren**.

Wählen Sie zum Ändern der Scan-Parameter im Kontextmenü (über Anklicken mit der rechten Maustaste) den Befehl **Eigenschaften**. Nun können Sie die Einstellungen des Scanauftrags beliebig verändern.



Periodischer Scanauftrag: Mit dieser Funktion lassen sich Scanaufträge für einzelne Rechner oder Rechnergruppen definieren. Im Konfigurationsdialog lassen sich auf den jeweiligen Karteireitern Wiederholungsintervall, Analyseumfang und weitere Scaneinstellungen festlegen. Erfahren Sie mehr zu den Einstellungsmöglichkeiten für Scanaufträge im Kapitel **Scanaufträge definieren**.

Wählen Sie zum Ändern der Scan-Parameter im Kontextmenü (über Anklicken mit der rechten Maustaste) den Befehl **Eigenschaften**. Nun können Sie die Einstellungen des Scanauftrags beliebig verändern.



Backup-Auftrag: Definieren Sie hier, wann und in welchem Umfang die Daten auf Clients gebackupt werden sollen. Erfahren Sie mehr zu den Einstellungsmöglichkeiten für Scanaufträge im Kapitel **Backupaufträge definieren**.



Wiederherstellungsauftrag: Mit dieser Funktion lassen sich auf Clients oder Gruppen zentral Backups zurückspielen. Erfahren Sie mehr zu den Einstellungsmöglichkeiten für Scanaufträge im Kapitel **Backupaufträge definieren**.



Softwareerkennungsauftrag: Mit dieser Funktion lässt sich auf Clients oder Gruppen installierte Software ermitteln. Erfahren Sie mehr zu den Einstellungsmöglichkeiten für Softwareerkennungs-Aufträge im Kapitel **Softwareerkennung definieren**.



Softwareverteilungsauftrag: Mit dieser Funktion lässt sich auf Clients oder Gruppen installierte Software ermitteln. Erfahren Sie mehr zu den Einstellungsmöglichkeiten für Softwareerkennungs-Aufträge im Kapitel **Softwareverteilung definieren**.



Scanaufträge erneut (sofort) ausführen: Wählen Sie diese Funktion, um **einmalige Scanaufträge**, die bereits durchgeführt oder abgebrochen wurden, erneut auszuführen. Bei periodischen Scanaufträgen bewirkt diese Funktion, dass sie unabhängig vom Zeitplan sofort ausgeführt werden.



Protokolle: Rufen Sie mit dieser Funktion die Protokolle zu den Aufträgen des jeweiligen Clients auf.



Alle Aufträge anzeigen



Nur Scan-Aufträge anzeigen



Nur Backup-Aufträge anzeigen



Nur Wiederherstellungsaufträge anzeigen



Nur Softwareerkennungsaufträge anzeigen



Nur Softwareverteilungsaufträge anzeigen



Nur Rollbackaufträge anzeigen



Nur einmalige Scanaufträge anzeigen



Nur periodische Scanaufträge anzeigen



Nur offene Scanaufträge anzeigen



Nur erledigte Scanaufträge anzeigen

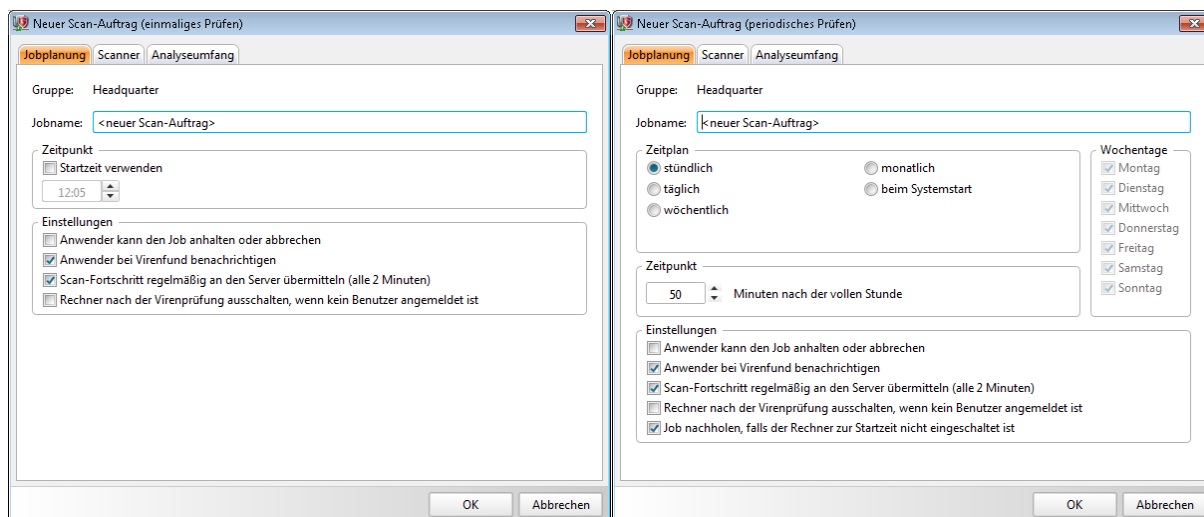


Gruppenjobs ausführlich anzeigen: Zeigt bei Gruppenjobs alle zugehörigen Einträge an. Die Option ist nur verfügbar, wenn in der Computerliste eine Gruppe selektiert ist.

Scanaufträge definieren

Jobplanung

Hier kann festgelegt werden, welchen Namen der Scanauftrag haben soll. Hier sollten aussagekräftige Namen, wie *Archivprüfung* oder *Monatliche Prüfung* Verwendung finden, um den gewünschten Job eindeutig zu charakterisieren und in der tabellarischen Übersicht wiederzufinden. Darüber hinaus können den Anwendern Berechtigungen zum Anhalten oder Abbrechen des Jobs über das Kontextmenü des Trays eingeräumt werden. Über die Option **Scan-Fortschritt regelmäßig an den Server übermitteln** können Sie sich im G Data Administrator den Fortschritt eines laufenden Scanauftrags auf einem Client in Prozent anzeigen lassen. Mit der Funktion **Rechner nach der Virenprüfung ausschalten, wenn kein Benutzer angemeldet ist** haben Sie eine weitere Option, die Ihnen hilft, den administrativen Aufwand zu verringern. Sollte ein Rechner zum festgelegten Zeitpunkt eines Scanauftrags nicht eingeschaltet sein, kann über die Option **Job nachholen, falls der Rechner zur Startzeit nicht eingeschaltet ist**, der Scanauftrag gestartet werden, wenn der Rechner nach diesem Zeitpunkt hochgefahren wird.



Bei einmaligen Scanaufträgen können Sie eine Startzeit definieren, bei periodischen Scanaufträgen können Sie festlegen, wann und in welchem Rhythmus die Virenprüfung erfolgen soll. Wird **Beim Systemstart** ausgewählt, fallen die Vorgaben der Zeitplanung weg und die G Data Software führt die Prüfung aus, wenn der Rechner neu gestartet wird.

Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** bestimmen, dass der Rechner nur an Werktagen eine Virenprüfung durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird.

Wird ein **einmaliger Scanauftrag** angelegt, steht nur die Option **Startzeit verwenden** zur Verfügung. Ohne Angabe einer Startzeit wird der Scanauftrag sofort nach dem Anlegen gestartet.

Scanner

In dem Scanner-Menü lassen sich die Einstellungen vornehmen, mit denen der Scanauftrag ausgeführt werden soll. Die folgenden Optionen sind verfügbar:

- **Engines benutzen:** Die G Data Software arbeitet mit zwei unabhängig voneinander operierenden Virenanalyseeinheiten. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenbekämpfung. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich; d.h. wenn Sie nur eine Engine verwenden, kann der Analysevorgang schneller erfolgen. Wir empfehlen die Einstellung **Beide Engines - performance-optimiert**. Hierbei sind beide Virens Scanner so miteinander verwoben, dass sie die optimale Erkennung mit minimierter Scandauer ermöglichen.
- **Im Fall einer Infektion:** Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Je nachdem, für welche Zwecke der jeweilige Clientrechner verwendet wird, sind hier unterschiedliche Einstellungen sinnvoll. Bei der Einstellung **Datei in Quarantäne verschieben** wird eine infizierte Datei in ein spezielles Verzeichnis verschoben, welches der G Data ManagementServer anlegt. Dort werden infizierte Dateien verschlüsselt, sodass etwaige Schadfunktionen nicht mehr ausgeführt werden können. Dateien in der **Quarantäne** können vom Netzwerkadministrator desinfiziert, gelöscht, an den Ursprungsort zurückbewegt oder gegebenenfalls an die **Internet-Ambulanz** gesandt werden.

- **Infizierte Archive:** Legen Sie hier fest, wie infizierte **Archive** behandelt werden sollen. Beachten Sie beim Festlegen dieser Einstellungen, dass ein Virus innerhalb eines Archives erst dann Schaden anrichtet, wenn das Archiv entpackt wird.
- **Dateitypen:** Hier können Sie festlegen, welche Dateitypen von G Data auf Viren untersucht werden sollen. Beachten Sie, dass eine Überprüfung aller Dateien eines Computers eine gewisse Zeit in Anspruch nehmen kann.
- **Priorität Scanner:** Über die Stufen **hoch**, **mittel** und **niedrig** können Sie festlegen, ob eine Virenprüfung durch G Data auf Ihrem System hohe Priorität haben soll (in diesem Fall erfolgt die Analyse schneller, allerdings sind Performanceeinbußen bei anderen Anwendungen möglich) oder niedrige Priorität (die Analyse benötigt mehr Zeit, dafür werden andere Anwendungen nicht beeinträchtigt). Je nach der Zeit, zu der Sie die Virenanalyse durchführen, sind hier unterschiedliche Einstellungen sinnvoll.
- **Einstellungen:** Legen Sie hier fest, welche zusätzlichen Virenanalysen die G Data Software durchführen soll. Die hier gewählten Optionen sind für sich gesehen durchaus sinnvoll, je nach Anwendungsart kann der Vorteil der Zeitersparnis durch Weglassen dieser Überprüfungen das etwas geringere Maß an Sicherheit aufwiegen. Folgende Einstellungsmöglichkeiten stehen Ihnen hier zur Verfügung:

Heuristik: In der Heuristik werden Viren nicht nur anhand der Virendatenbanken, sondern auch anhand bestimmter virentypischer Merkmale ermittelt. Die Heuristik kann in sehr seltenen Fällen einen Fehlalarm erzeugen.

Archive: Das Überprüfen gepackter Daten in Archiven ist sehr zeitintensiv und kann in der Regel unterbleiben, wenn der **G Data Wächter** auf dem System aktiv ist. Dieser erkennt dann beim Entpacken des Archives einen bis dahin verborgenen Virus und unterbindet automatisch dessen Verbreitung. Dennoch sollten bei regelmäßigen Kontrollen, außerhalb der eigentlichen Nutzungszeit des Computers, auch eine Prüfung der Archive erfolgen.

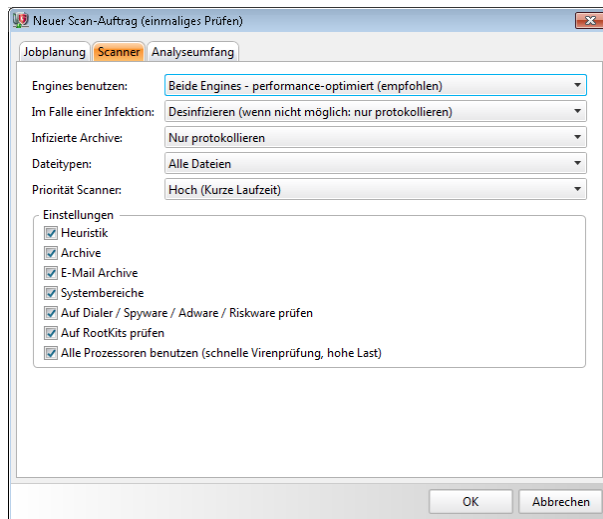
E-Mail Archive: Das Überprüfen von E-Mail Archiven ist sehr zeitintensiv und kann in der Regel unterbleiben, wenn der **G Data Wächter** bzw. das Outlook-Plugin auf dem System aktiv ist. Der Wächter erkennt beim Zugriff auf das Archiv einen bis dato verborgenen Virus und unterbindet automatisch dessen Verbreitung. Dennoch sollten bei regelmäßigen Kontrollen, außerhalb der eigentlichen Nutzungszeit des Computers, auch eine Kontrolle der Archive erfolgen.

Systembereiche: Die Systembereiche Ihres Computers (**Bootsektoren, Master Boot Record etc.**) die eine grundlegende Basis für das Betriebssystem bieten, sollten nicht von der Virenkontrolle ausgeschlossen werden, da sich einige Schädlinge speziell in diesem Bereich des Systems einnisten können.

Auf Dialer / Spyware / Adware / Riskware prüfen: Mit der G Data Software können Sie Ihr System auch auf **Dialer** und andere Schadprogramme (**Spyware, Adware, Riskware**) überprüfen. Hierbei handelt es sich z.B. um Programme, die unerwünschte teure Internetverbindungen aufbauen und in ihrem wirtschaftlichen Schadpotential dem Virus in nichts nachstehen. Spyware kann z.B. Ihr Surfverhalten oder sogar sämtliche Tastatureingaben (und damit auch Ihre Passwörter) unbemerkt speichern und bei nächster Gelegenheit über das Internet an fremde Personen weiterleiten.

Auf RootKits prüfen: Ein **Rootkit** versucht, sich herkömmlichen Virenerkennungsmethoden zu entziehen. Sie können mit dieser Funktion gezielt nach Rootkits suchen, ohne eine komplette Überprüfung der Festplatten und gespeicherten Daten vorzunehmen.

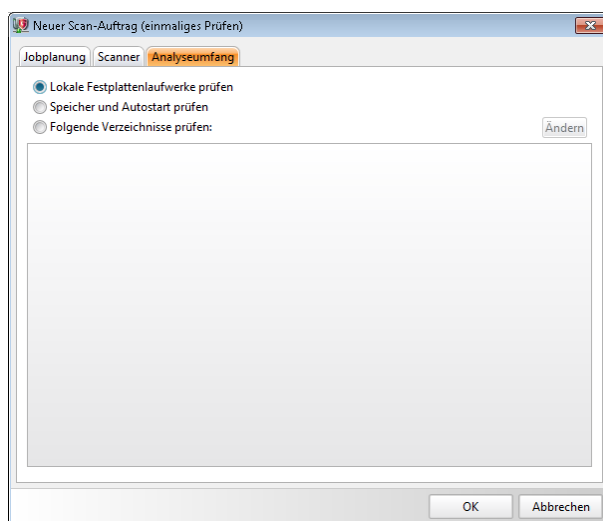
Alle Prozessoren benutzen: Mit dieser Option können Sie die Virenprüfung bei Systemen mit mehreren **Prozessorkernen** auf alle Prozessoren verteilen und auf diese Weise die Virenprüfung deutlich schneller durchführen. Nachteil dieser Option ist, dass so weniger Rechenleistung für andere Anwendungen verfügbar ist. Diese Option sollte nur dann genutzt werden, wenn der Scanauftrag zu Zeiten durchgeführt werden, zu denen das System nicht regulär genutzt wird (z.B. nachts).



Analyse-Umfang

Über das Register **Analyse-Umfang** lässt sich beim Client die Virenkontrolle auch auf bestimmte Verzeichnisse begrenzen. Auf diese Weise können z.B. Ordner mit selten benötigten Archiven ausgespart und in einem separaten Scanauftrag geprüft werden. Die Verzeichnisauswahl bezieht sich dabei auf den aktuell ausgewählten Rechner und nicht auf den gewählten Client.

Besonderheit bei Scanaufträgen auf einem Linux-Fileserver: Bei der Verzeichnisauswahl werden das Root-Laufwerk (/) und alle Freigaben zurück geliefert. So können Scanaufträge gezielt auf ausgewählten Freigaben oder beliebig gewählten Verzeichnissen des Dateiservers durchgeführt werden.



Backupaufträge definieren

Jobplanung

Hier kann festgelegt werden, welchen Namen der Backupauftrag haben soll. Hier sollten aussagekräftige Namen, wie *Monatsbackup* oder *Teilbackup Außendienst* Verwendung finden, um den gewünschten Job eindeutig zu charakterisieren und in der tabellarischen Übersicht wiederzufinden. Sie können hier festlegen, wann und in welchem Rhythmus das Backup erfolgen soll und ob es sich dabei um ein **Teilbackup** oder **Vollbackup** handelt. Beim Teilbackup werden nur die Daten gebackupt, die sich seit dem letzten Teil- oder Vollbackup geändert haben. Dies spart Zeit bei der Erstellung des Backups, die Wiederherstellung ist im Fall eines Zurückspiels von Daten allerdings langwieriger, da aus den verschiedenen Teilbackupdatenbeständen das letzte Systemabbild rekonstruiert werden muss.

Um Probleme zu vermeiden, die sich beim Abschalten eines nicht ans Stromnetz angeschlossenen Notebooks ergeben, können Sie die Einstellung **Nicht im Batteriebetrieb ausführen** auswählen. Backups von mobilen Geräten erfolgen dann nur, wenn diese auch ans Stromnetz angeschlossen sind.

Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** bestimmen, dass der Rechner nur an Werktagen eine Backup durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird.

The screenshot shows the 'Backup-Auftrag' dialog box with the 'Jobplanung' tab selected. The 'Datei-/Verzeichnisauswahl' (File/Directory Selection) sub-tab is active. The 'Gruppe' (Group) is set to 'Headquarter' and the 'Jobname' is '<neuer Backup-Auftrag>'. Under 'Vollbackup(s)' (Full backup(s)), the 'Zeitplan' (Schedule) is set to 'täglich' (daily). The 'Wochentage' (Days of the week) are all checked: Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, and Sonntag. The 'Zeitpunkt' (Time) is set to '25.09.2012 um 15:02'. The 'Einstellungen' (Settings) section has 'Nicht im Batteriebetrieb ausführen' (Do not run in battery mode) checked. Under 'Teilbackup(s)' (Partial backup(s)), the 'Zeitplan' is set to 'täglich'. The 'Wochentage' are all checked. The 'Zeitpunkt' is set to '15:02'. The 'Einstellungen' section has 'Nicht im Batteriebetrieb ausführen' checked. At the bottom are 'OK' and 'Abbrechen' buttons.

Über die Registerkarte **Datei-/Verzeichnisauswahl** können Sie festlegen, welchen Daten genau bei den einzelnen Clients/Gruppen vom Backup erfasst werden sollen. Im Bereich **Backup-Umfang** können Sie dazu direkt im Verzeichnisbaum des jeweiligen Clients die Ordner festlegen, die gesichert werden sollen.

Über die Häkchen unter **Dateien ausschließen** können Sie generell Dateien und Ordner mit bestimmten Attributen (z.B. temporäre Ordner und Dateien, Systemdateien) vom Backup ausschließen. Darüber hinaus können Sie auch individuelle Ausnahmen definieren, indem Sie die Endung bestimmter Dateitypen auf die Ausnahmeliste setzen.

The screenshot shows the 'Backup-Auftrag' dialog box with the 'Datei-/Verzeichnisauswahl' sub-tab selected. The 'Backup-Umfang' (Backup Scope) section shows a tree view of the file system with a 'Bearbeiten...' button. The 'Dateien ausschließen' (Exclude files) section has several checked items: 'Temporärverzeichnisse mit Dateien', 'Temporäre Internetverzeichnisse mit Dateien', 'Thumbs.db', 'Temporäre Dateien (Dateiattribut)', and 'Systemdateien (Dateiattribut)'. There is a 'Dateitypen: *' field with 'Hinzufügen' and 'Löschen...' buttons. The 'Zwischenspeicher' (Intermediate storage) section has 'Clientabhängigen Standardpfad verwenden' checked. The 'Verzeichnis:' field is empty. At the bottom are 'OK' and 'Abbrechen' buttons.

Softwareerkennung definieren

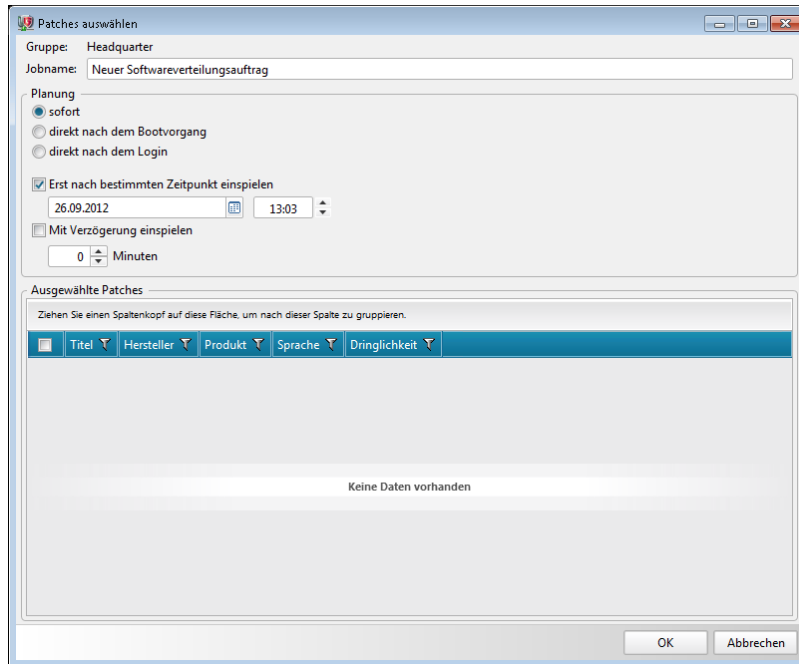
Mit dieser Funktion lässt sich auf Clients oder Gruppen die Anwendbarkeit von verfügbaren **Patches** ermitteln. Die Ausführung der Softwareerkennung kann dabei **zeitgesteuert** oder **sobald verfügbar** erfolgen. Wählen Sie aus, ob Sie die Anwendbarkeit von Software-Patches anhand von Merkmalen ermitteln möchten oder gezielt nach spezifischen Patches oder nur kritischen Patches suchen.

Geben Sie die Merkmale der Software an, die Sie erkennen möchten. Um bestimmte Merkmale (Hersteller, Produktname, Dringlichkeit, Sprache, Sicherheitsrelevanz) als Auswahlkriterium zuzulassen, setzen Sie bitte das Häkchen beim jeweiligen Merkmal. So können Sie z.B. Software nur von bestimmten Herstellern ermitteln oder konkrete Programmversionen einer Software. Wildcards wie "?" und "*" zur Filterung sind dabei zulässig.

Softwareverteilung definieren

Hier können Sie festlegen wann ausgewählte Patches, die anwendbar sind, auf den Clients und Gruppen installiert werden sollen. Dabei können Sie festlegen, dass die Patches sofort, direkt nach dem Bootvorgang oder Login oder erst zu einem bestimmten Zeitpunkt eingespielt werden sollen.

Über die Einstellung bei Mit Verzögerung einspielen können Sie das Einspielen von Patches zeitlich vom Bootvorgang trennen. Vorteil hierbei: Bootvorgang und Patcheinspielung beeinträchtigen nicht beide gleichzeitig die Performance des Clients.



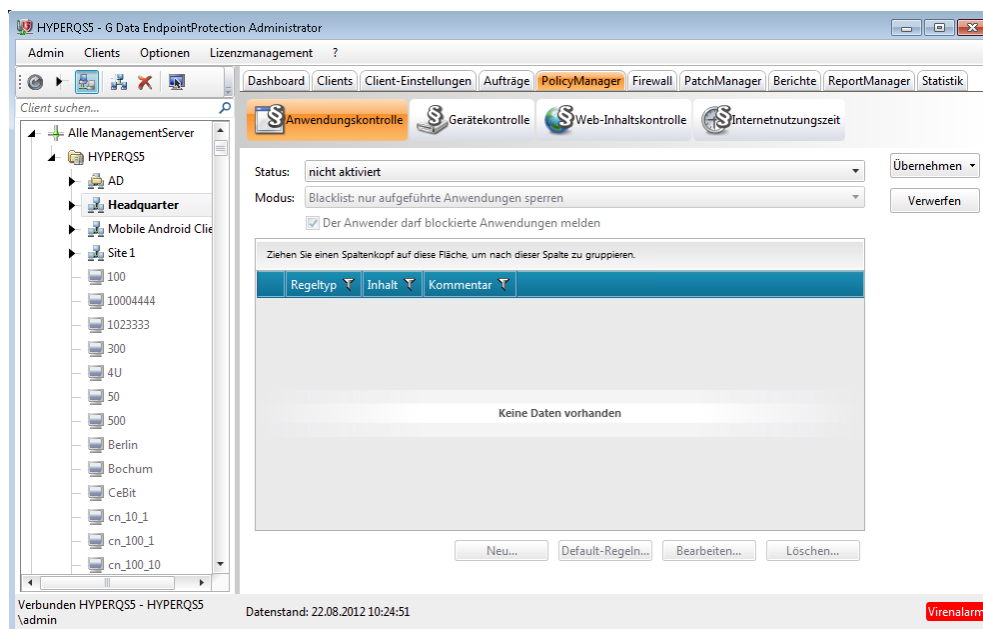
PolicyManager

Der PolicyManager enthält eine Anwendungs-, Geräte-, Web-Inhaltskontrolle sowie eine Überwachung der Internetnutzungszeit. Diese Funktionen erlauben eine flächendeckende Umsetzung der Unternehmensrichtlinien zur Nutzung der firmeneigenen PCs. So kann über den PolicyManager bestimmt werden, ob und in welchem Umfang externe Massenspeicher- oder optische Medien genutzt werden können. Ebenso lässt sich definieren, welche Webseiten innerhalb welches Zeitrahmens besucht und welche Programme auf den Firmen-PCs genutzt werden dürfen.

Anwendungskontrolle

Mit der Anwendungskontrolle lassen sich bestimmte Programme für die Nutzung durch ausgewählte Clients sperren. Legen Sie dazu unter **Status** fest, ob die Einschränkungen für alle Benutzer des jeweiligen Clients gelten sollen oder nur für Benutzer, die keine Administratorberechtigungen auf dem Client-Rechner besitzen. Unter **Modus** bestimmen Sie nun, ob es sich bei der Anwendungskontrollliste um eine Whitelist oder Blacklist handeln soll.

- **Whitelist:** Nur die hier aufgeführten Anwendungen können vom Client-Rechner aus verwendet werden.
- **Blacklist:** Hier aufgeführte Anwendungen können auf dem Client-Rechner nicht verwendet werden.



Neue Regel erstellen

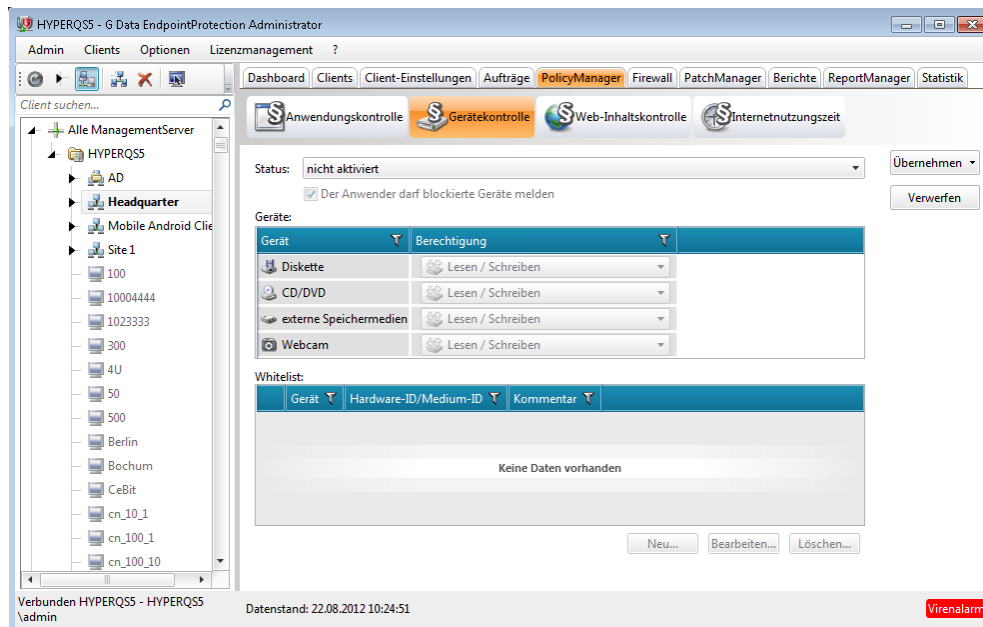
Über die **Neu...**-Schaltfläche, kann eine neue Regel erstellt werden. Zur Auswahl stehen die Regeltypen **Hersteller**, **Datei** und **Verzeichnis**.

- **Hersteller:** Hier werden die Herstellerinformationen in Programmdateien dazu verwendet, eine Nutzung dieser Anwendungen zu erlauben oder zu verbieten. Sie können den Namen des Herstellers hier entweder selbst eintragen oder über die **Hersteller suchen...** - Schaltfläche gezielt eine Datei auswählen, aus der die Herstellerinformation ausgelesen und übernommen wird.
- **Datei:** Hier können Sie bestimmte Programmdateien für den jeweiligen Client sperren oder erlauben. Dabei können Sie entweder den Dateinamen eingeben, um den Zugriff auf Dateien dieses Namens generell zu verbieten/zu erlauben oder Sie klicken auf die Schaltfläche **Merkmale einer Datei ermitteln...**, um ganz speziell eine bestimmte Datei anhand ihrer Merkmale zu definieren. Bei Bedarf können Sie als Platzhalter für beliebige Inhalte einen Stern (*) am Anfang und/oder Ende der Merkmale Dateiname, Produktname und Copyright verwenden.
- **Verzeichnis:** Über diese Funktion können Sie komplette Verzeichnisse (auf Wunsch inklusive der jeweiligen Unterverzeichnisse) für Clients freigeben oder sperren.

Gerätekontrolle

Mit Hilfe der Gerätekontrolle lässt sich der Zugriff auf externe Speichermedien begrenzen. So können USB-Sticks von der Nutzung ausgeschlossen, CD/DVD-Laufwerke mit Schreib- oder Leserechten ausgestattet und auch die Verwendung von Kameras eingeschränkt werden.

Unter **Status** können Sie festlegen, ob die Einschränkungen für alle Benutzer des jeweiligen Clients gelten sollen oder nur für Benutzer, die keine Administratorberechtigungen auf dem Client-Rechner besitzen.



Für jeden Client werden unter **Geräte** die Geräteklassen angezeigt, deren Nutzung eingeschränkt werden kann. Diese müssen nicht zwangsläufig auch am jeweiligen Client vorhanden sein. So können zum Beispiel für ausgewählte Nutzergruppen generell die Nutzung von Diskettenlaufwerken untersagt werden, unabhängig davon, ob die jeweiligen Rechner ein Diskettenlaufwerk besitzen oder nicht. Folgende Berechtigungen lassen sich definieren:



Lesen / Schreiben: Es besteht voller Zugriff auf das Gerät.



Lesen: Medien können nur gelesen werden, ein Abspeichern von Daten ist nicht erlaubt.



Zugriff verbieten: Sowohl Lese- als auch Schreibzugriffe auf das Gerät sind nicht erlaubt. Das Gerät kann vom Anwender nicht verwendet werden.

Whitelist

Über die Whitelist-Einstellungen können Sie die Gerätenutzung, die Sie für den Client-Nutzer in irgendeiner Weise eingeschränkt haben (**Lesen / Zugriff verbieten**) mit bestimmten Einschränkungen wieder erlauben. Wenn Sie auf die **Neu...**-Schaltfläche klicken, öffnet sich ein Dialogfenster, in dem die Geräte mit Nutzungseinschränkungen angezeigt werden. Wenn Sie nun auf **[...]** klicken, können Sie für bestimmte Geräte eine Ausnahme zulassen.

- **Medium-ID verwenden:** Hier können Sie z.B. festlegen, dass nur bestimmte CDs oder DVDs mit einem CD/DVD-Laufwerk genutzt werden können (z.B. spezielle Firmen-Präsentationen auf CD).
- **Hardware-ID verwenden:** Hier können Sie z.B. festlegen, dass nur bestimmte USB-Sticks verwendet werden dürfen. Bei Hardware-ID-basierten Freigaben für einzelne Speichergeräte hat der Netzwerkadministrator die Möglichkeit, zu kontrollieren, welche Mitarbeiter die Möglichkeit zur Weitergabe von Daten haben.

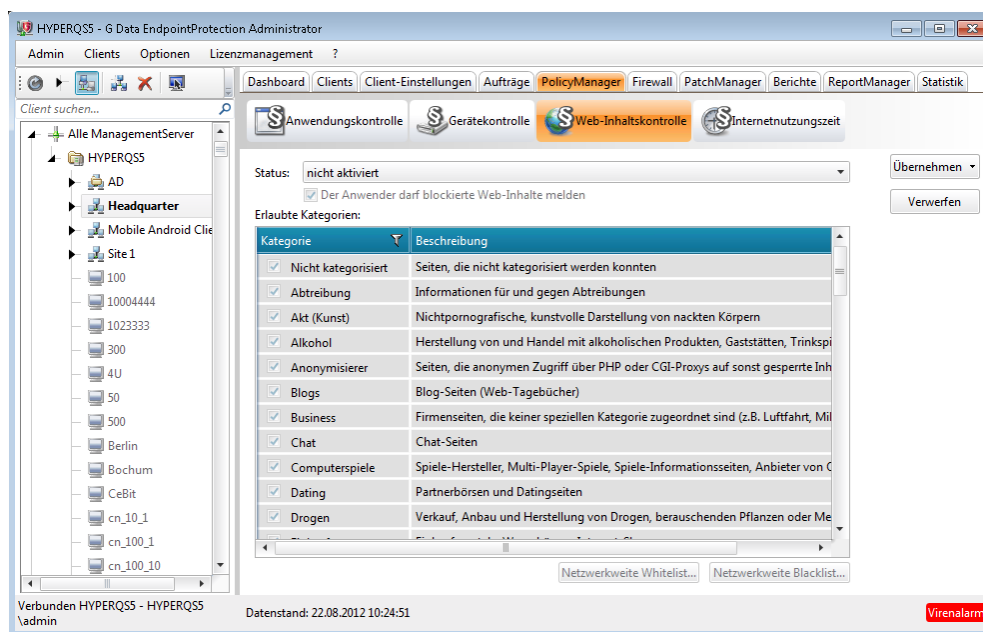
Um eine Medium-ID oder Hardware-ID zu ermitteln, klicken Sie im Dialogfeld **Hardware-ID/ Medium-ID ermitteln** auf den Eintrag **Client** und wählen dort den Client aus, auf dem sich das freizugebende Medium befindet. Die entsprechende ID wird dann automatisch ausgelesen.

Über die lokale Suche können Sie die ID des Mediums oder der Hardware mit Hilfe des Rechners ermitteln, auf dem der G Data ManagementServer installiert ist. Das Medium muss dazu an die entsprechende Maschine angeschlossen bzw. dort eingelegt sein.

Web-Inhaltskontrolle

Die Web-Inhaltskontrolle dient dazu, Anwendern zwar den dienstlichen Zugang zum Internet zu erlauben, aber das Surfen auf nicht erwünschten Websites oder in bestimmten Themenbereichen zu unterbinden. Nach der Auswahl des zu bearbeitenden Clients auf der rechten Seite der Programmoberfläche, können Sie hier gezielt Bereiche durch Setzen eines Häkchens für den jeweiligen Client erlauben oder durch Entfernen des Häkchens verbieten. Die Kategorien decken dabei eine große Anzahl thematischer Bereiche ab und werden von G Data laufend aktualisiert. Somit entfällt für den Netzwerkadministrator der mit der Pflege von White- und Blacklists verbundene Aufwand.

Unter **Status** können Sie festlegen, ob die Einschränkungen für alle Benutzer des jeweiligen Clients gelten sollen oder nur für Benutzer, die keine Administratorenrechte auf dem Client-Rechner besitzen.



Netzwerkweite Whitelist

Mit der **netzwerkweiten Whitelist** können unabhängig von den Einstellungen, die unter **Erlaubte Kategorien** vorgenommen wurden, bestimmte Webseiten unternehmensweit für das gesamte Netzwerk freigegeben werden. Dies kann z.B. die Webpräsenz Ihres Unternehmens sein. Geben Sie dazu unter **URLs** die Adresse ein, die freigegeben werden soll, klicken Sie dann auf die Schaltfläche **Hinzufügen** und die entsprechende Seite ist freigegeben.

Netzwerkweite Blacklist

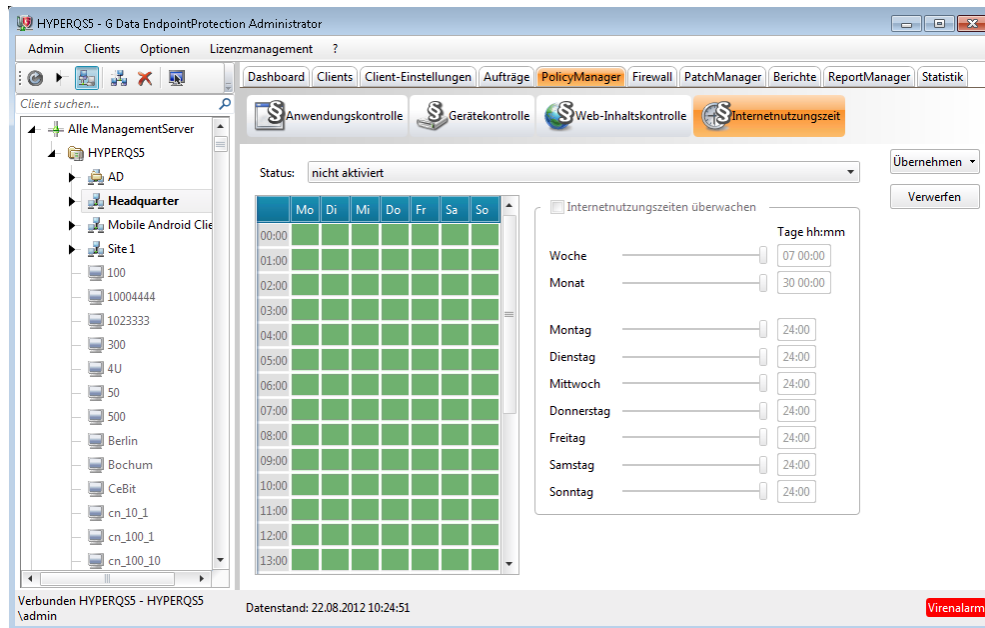
Mit der **netzwerkweiten Blacklist** können unabhängig von den Einstellungen, die unter **Erlaubte Kategorien** vorgenommen wurden, bestimmte Webseiten unternehmensweit für das gesamte Netzwerk gesperrt werden. Geben Sie dazu unter **URLs** die Adresse ein, die gesperrt werden soll, klicken Sie dann auf die Schaltfläche **Hinzufügen** und die entsprechende Seite ist gesperrt.

Internetnutzungszeit

Im Bereich **Internetnutzungszeit** kann die generelle Nutzung des Internets auf bestimmte Zeiten beschränkt werden. Zudem ist auch die Einrichtung eines Zeitkontingents für die Internetnutzung möglich. Unter **Status** wird festgelegt, ob die Einschränkungen für alle Benutzer des jeweiligen Clients gelten sollen oder nur für Benutzer, die keine Administratorberechtigungen auf dem Client-Rechner besitzen. Auf der rechten Seite kann über die dort vorhandenen Schieberegler das Kontingent festgelegt werden, dass auf dem jeweiligen Clientrechner für die Nutzung des Internets zur Verfügung steht. Es können tägliche, wöchentliche oder monatliche Kontingente vergeben werden; beispielsweise entspricht die Angabe **04/20:05** einer Internetnutzungszeit von 4 Tagen, 20 Stunden und 5 Minuten.

Im Zusammenspiel der Angaben zur Internetnutzung zählt immer der jeweils kleinste Wert. Wenn Sie also für den Monat eine zeitliche Beschränkung von vier Tagen festlegen, in der Woche aber z.B. fünf Tage erlauben, deckelt die Software die Internetnutzung für den Benutzer automatisch auf vier Tage.

Wenn der jeweilige Benutzer versucht, über das erlaubte Zeitkontingent hinaus auf das Internet zuzugreifen, erscheint im Browser ein Info-Bildschirm, der ihn darüber informiert, dass er sein Zeitkontingent überschritten hat. Im Bereich **Sperrzeiten** können Sie - zusätzlich zur zeitlichen Eingrenzung der Internetnutzung - bestimmte Zeiträume sperren. Gesperrte Zeiträume sind dabei rot dargestellt, freigegebene Zeiträume in grün. Um einen Zeitraum freizugeben oder zu sperren, markieren Sie diesen mit der Maus. Dann erscheint neben dem Mauszeiger ein Kontextmenü, in dem Sie zwei Möglichkeiten haben: **Zeit freigeben** und **Zeit sperren**. Wenn der jeweilige Benutzer versucht, während der gesperrten Zeiten auf das Internet zuzugreifen, erscheint im Browser ein Info-Bildschirm, der ihn darüber informiert, dass er zu diesem Zeitpunkt keinen Zugriff auf das Internet hat.



Firewall

In diesem Bereich kann die Firewall auf den jeweiligen Clients oder Gruppen zentral administriert werden. **Übersicht** gibt dem Systemadministrator eine Übersicht über den aktuellen Status der Firewall auf den installierten Clients, **Regelsätze** bietet Möglichkeiten zum Erstellen und Verwalten von Regelsätzen.

Übersicht

In der Übersicht werden alle Client-Rechner oder die Clients einer ausgewählten Gruppe angezeigt. Hier sehen Sie auf einen Blick, welche Einstellungen die jeweilige Client-Firewall hat und können durch Anklicken des jeweiligen Clients direkt Änderungen vornehmen.

Regelsatz oder Autopilot?

Es gibt zwei grundsätzlich verschiedene Möglichkeiten, eine Firewall zu betreiben.

- **Autopilot:** Wenn die Firewall auf "Autopilot" betrieben wird, ist sie schon standardmäßig von **G Data** vorkonfiguriert, erfüllt Ihre Aufgabe im Hintergrund und stört den Anwender nicht mit Rückfragen. Im Autopilotmodus optimiert die Firewall ihren Regelsatz mit der Zeit selbstständig.
- **Regelsatz:** Als Administrator können Sie auch individuelle Firewallregeln für unterschiedliche Rechner definieren.

Folgende Informationen hält die Übersichtsliste bereit:

- **Rechner:** Der Name des Client-Rechners. Anhand des abgebildeten Symbols können Sie hier erkennen, ob die Client-Software auf diesem Client installiert ist.
- **Firewall:** Hier erfahren Sie, ob die Firewall auf dem Client eingeschaltet, ausgeschaltet oder ggf. gar nicht installiert ist.
- **Autopilot / Regelsatz:** Sie können verschiedenen Clients unterschiedliche Firewall-Modi zuordnen (siehe oben).
- **Offsite-Konfiguration:** Wenn Sie für einen Client die Offsite-Konfiguration auswählen, kann der Anwender auf diesem Client seine Firewall-Einstellungen individuell verwalten und einstellen, solange er nicht mit dem Netzwerk des G Data ManagementServers verbunden ist. Die Offsite-Konfiguration kann nur verwendet werden, wenn die Firewall im Firmennetz nicht im Autopilot-Modus betrieben wird.

Um die Firewall-Einstellungen für die in der Liste ausgewählten Clients zu ändern, klicken Sie den Eintrag mit der rechten Maustaste an. Es öffnet sich ein Auswahlménü mit folgenden Optionen:

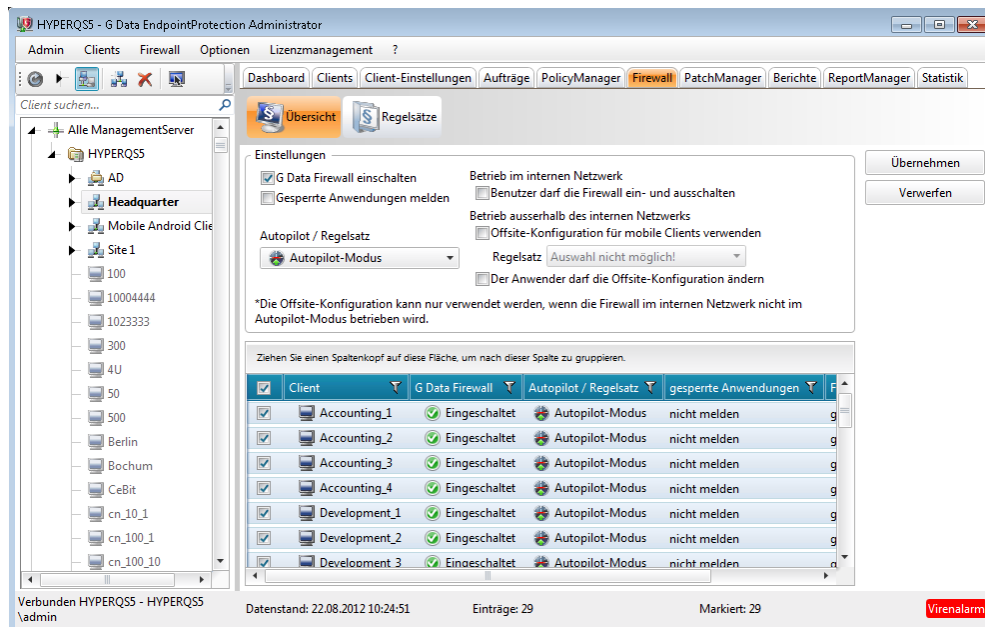
- **Regelsatz erstellen:** Hiermit wechseln Sie in den Bereich **Regelsätze** und können individuelle Regeln für ihre Client-Firewalls definieren.
- **Regelsatz bearbeiten:** Hiermit wechseln Sie in den Bereich **Regelsätze** und können bestehende Regeln für ihre Client-Firewalls ändern.
- **Firewall installieren:** Über diese Funktion können Sie auf aktivierten Client-Rechnern zentral eine Firewall installieren und im Anschluss administrieren.
- **Firewall deinstallieren:** Mit dieser Funktion wird die bestehende Client-Firewall deinstalliert.

Firewall-Einstellungen

Firewall einschalten: Durch Setzen des Häkchens wird die Firewall auf dem jeweiligen Client aktiviert. Wenn Sie das Häkchen entfernen, ist die Firewall inaktiv.

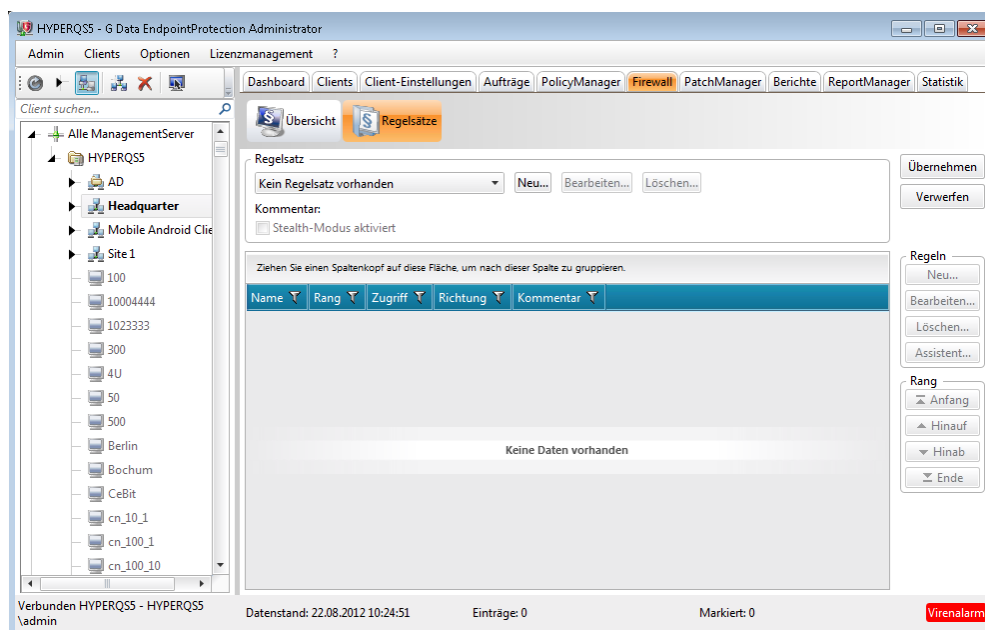
- **Gesperrte Anwendungen melden:** Wenn dieses Häkchen gesetzt ist und der Client-Rechner mit dem G Data ManagementServer verbunden ist, erhält der Systemadministrator im Bereich **Berichte** Informationen über Anwendungen, die durch die jeweilige Client-Firewall geblockt wurden.
- **Benutzer darf die Firewall ein- und ausschalten:** Hier können Sie als Netzwerkadministrator dem Nutzer des Client-Rechners erlauben, die Firewall zwischenzeitlich auszuschalten. Diese Möglichkeit ist nur dann gegeben, solange sich der Client innerhalb des Firmennetzwerks befindet und sollte natürlich nur versierten Anwendern ermöglicht werden.
- **Offsite-Konfiguration für mobile Clients verwenden:** In der **Offsite-Konfiguration** werden die Firewall-Regelsätze des Client-Rechners, die in Ihrem Firmennetzwerk gelten, durch Standardregelsätze ersetzt, die automatisch den Umgang mit dem Internet, sicheren-, unsicheren und zu blockierenden Netzen regeln. Auf diese Weise ist der mobile Rechner optimal geschützt, solange er sich nicht im Netzwerk des G Data ManagementServers befindet. Sobald der mobile Rechner wieder mit dem Netzwerk des G Data ManagementServers verbunden wird, werden diese Standardregelsätze automatisch wieder durch die Regelsätze ersetzt, wie Sie für diesen jeweiligen Client in Ihrem Netzwerk gelten.
- **Der Anwender darf Offsite-Konfiguration ändern:** Diese Option soll es versierten Anwendern erlauben, ihre Firewall außerhalb des Netzwerks individuell zu konfigurieren. Sobald der mobile Rechner wieder mit dem G Data ManagementServer verbunden wird, werden die durchgeführten Änderungen wieder durch die vom Netzwerkadministrator vorgegebenen Regeln für diesen Client ersetzt.

Die **Offsite-Konfiguration** kann nur verwendet werden, wenn die Firewall im Firmennetz nicht im **Autopilot-Modus** betrieben wird. Wenn der jeweilige Client im Firmennetzwerk die Autopilot-Einstellungen für die Firewall verwendet, werden die Autopilot-Einstellungen auch dann verwendet, wenn der Client nicht mit dem Netzwerk verbunden ist.



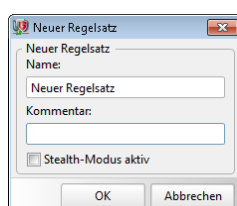
Regelsätze

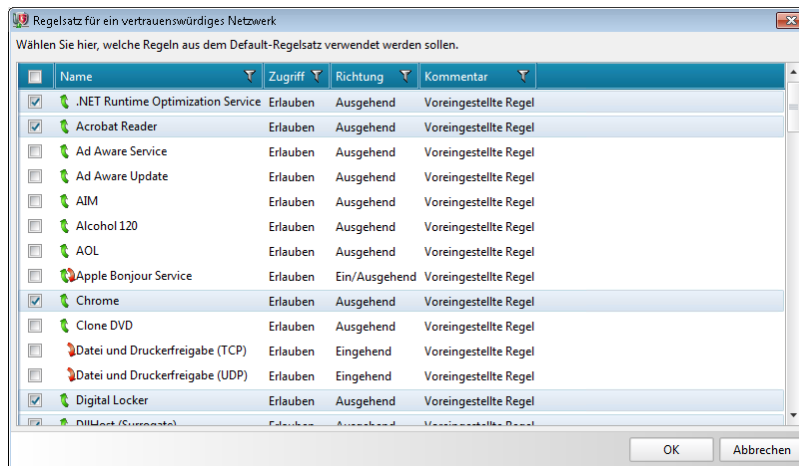
In diesem Bereich können Sie für verschiedene Netzwerke spezielle Regeln und Regelsätze erstellen.



Regelsatz erstellen

Klicken Sie bei **Regelsatz** auf die Schaltfläche **Neu** und Sie haben die Möglichkeit, aus einer großen Anzahl von Default-Regeln und ggf. selbst angelegten Regeln einen individuell auf den Client zugeschnittenen Regelsatz aufzustellen. In der Übersicht wird der jeweilige Regelsatz mit Namen und Stealth-Modus-Status angezeigt. Mit Hilfe der Schaltflächen **Neu**, **Löschen** und **Bearbeiten** können Sie bestehende Regelsätze verändern bzw. weitere Regelsätze hinzufügen.

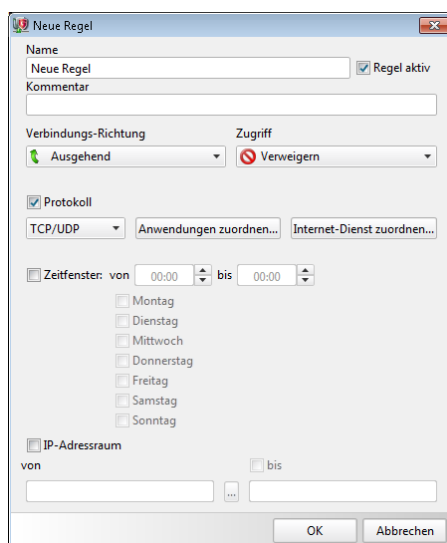




Mit dem **Stealth-Modus** (engl.: verborgen, unbemerkt) werden Anfragen an den Computer, die dazu dienen, die Erreichbarkeit von Ports zu überprüfen, nicht beantwortet. Dies erschwert es Angreifern, auf diese Weise Informationen über das System zu erhalten.

Regel erstellen

Wenn Sie individuelle Regeln erstellen möchten, die Sie dann als Teil eines Regelsatzes auf den Clients verwenden können, klicken Sie bei **Regeln** auf die Schaltfläche **Neu**.



Nun erscheint ein Dialog mit folgenden Einstellungsmöglichkeiten:

- **Name:** Hier findet sich bei voreingestellten und automatisch generierten Regeln der **Programmname** für den die jeweilige Regel zutrifft. Sie können den Namen über die **Bearbeiten...**-Schaltfläche auch jederzeit verändern oder um zusätzliche Informationen ergänzen.
- **Regel aktiv:** Sie können eine Regel durch Entfernen des Häkchens inaktiv setzen, ohne sie gleich zu löschen.
- **Kommentar:** Hier erfahren Sie, auf welche Weise die Regel erzeugt wurde. Bei für den Regelsatz voreingestellten Regeln steht **Voreingestellte Regel**, bei Regeln, die sich aus dem Dialog aus dem **Firewall-Alarm** ergeben steht **per Nachfrage generiert** und für Regeln, die Sie selber über den Profi-Dialog generieren, können Sie einen eigenen Kommentar einfügen.
- **Verbindungs-Richtung:** Mit der **Richtung** wird definiert, ob es sich bei dieser Regel um eine Regel für eingehende, ausgehende oder ein- und ausgehende Verbindungen handelt.
- **Zugriff:** Hier wird eingestellt, ob für das jeweilige Programm innerhalb dieses Regelsatzes der Zugriff erlaubt oder verweigert werden soll.

- **Protokoll:** Hier können Sie auswählen, welchen **Verbindungsprotokollen** Sie einen Zugriff erlauben oder verwehren wollen. Dabei haben Sie die Möglichkeit, Protokolle generell zu sperren oder freizugeben oder die Verwendung des Protokolls mit der Nutzung einer bestimmten Anwendung oder mehrerer Anwendungen zu verbinden (**Anwendungen zuordnen**). Genauso können Sie die unerwünschten bzw. erwünschten Ports über die Schaltfläche **Internet-Dienst zuordnen** genau definieren.
- **Zeitfenster:** Sie können den Zugriff auf Netzwerkressourcen auch zeitabhängig gestalten und so z.B. dafür sorgen, dass ein Zugriff nur zu Ihren Arbeitszeiten und nicht außerhalb dieser Zeiten erfolgt.
- **IP-Adressraum:** Gerade für Netzwerke mit fest vergebenen IP-Adressen macht es Sinn, deren Nutzung über eine Beschränkung des IP-Adressraumes zu reglementieren. Ein klar definierter IP-Adressraum verringert die Gefahr eines Angriffs deutlich.

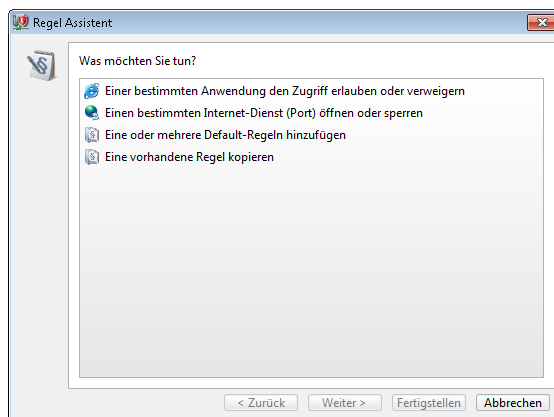
Auf diese Weise können Sie individuelle Regeln erstellen, die Sie dann für Ihre Regelsätze auswählen können.

Assistent nutzen

Mit dem Regel Assistenten können Sie auf einfache Weise zusätzliche Regeln für den jeweiligen Regelsatz definieren.

Mit dem Regel Assistenten verändern Sie eine oder mehrere Regeln in dem jeweils ausgewählten Regelsatz. Sie erstellen also immer eine Regel innerhalb eines Regelsatzes, der verschiedene Regeln beinhaltet.

Abhängig davon, welchen Regelsatz Sie für das jeweilige Netzwerk definiert haben, kann eine Anwendung in dem einen Regelsatz (z.B. für nicht vertrauenswürdige Netze) gesperrt sein, in dem anderen Regelsatz (z.B. für vertrauenswürdige Netze) vollen Netzzugriff haben. So könnten Sie z.B. einen Browser mit entsprechend unterschiedlichen Regeln so beschränken, dass er wohl auf Seiten zugreifen kann, die in ihrem Heimnetzwerk bereitstehen, aber keine Möglichkeit hat, auf Inhalte aus dem DFÜ-Netzwerk zuzugreifen.



Der Regel Assistent stellt folgende Aktionen zur Verfügung:

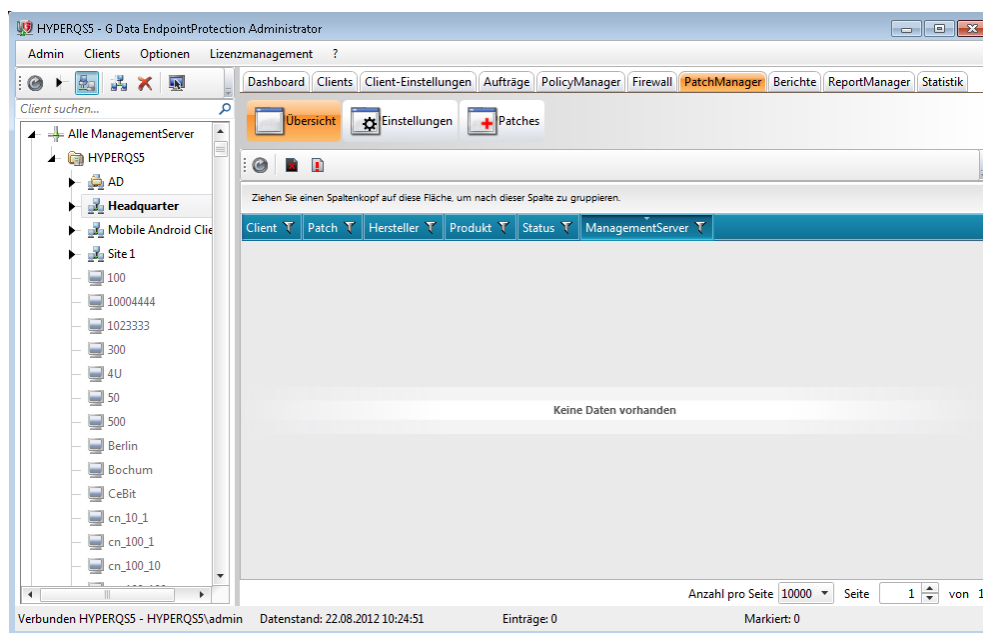
- **Einer bestimmten Anwendung den Zugriff erlauben oder verweigern:** Hiermit können Sie gezielt eine Anwendung auswählen und ihr im Rahmen des gewählten Regelsatzes den Zugriff auf das Netzwerk erlauben oder verbieten. Wählen Sie im Assistenten dazu einfach das gewünschte Programm aus (**Programmpfad**) und geben Sie dann unter **Verbindungsrichtung** an, ob das Programm für eingehende Verbindungen, ausgehende Verbindungen oder sowohl ein-, als auch ausgehende Verbindungen gesperrt werden soll. Auf diese Weise können Sie z.B. ihre MP3-Playersoftware ggf. daran hindern, Daten über Ihre Hörgewohnheiten weiterzugeben (ausgehende Verbindungen) oder dafür sorgen, dass nicht automatisch Programmupdates aufgespielt werden (eingehende Verbindungen).
- **Einen bestimmten Internet-Dienst (Port) öffnen oder sperren:** Im Assistenten haben Sie die Möglichkeit, Ports komplett zu sperren oder aber auch nur für eine bestimmte Anwendung (z.B. CRM-Software) freizugeben.
- **Eine oder mehrere Default-Regeln hinzufügen:** Bestimmen Sie hier, welche der angelegten Regeln als Default-Regel definiert wird. Default-Regeln werden automatisch vorgeschlagen, wenn ein neuer Regelsatz erstellt werden soll.

- **Eine vorhandene Regel kopieren:** Mit dieser Funktion können Sie zum weiteren Editieren eine Kopie einer bestehenden Regel anfertigen.

PatchManager

Mit dem PatchManager können Patches von Microsoft und anderen Softwareanbietern auf den Clients verteilt werden, darüber hinaus können auch Upgrades auf den Clients eingespielt werden.

Übersicht



In der Übersicht können Sie sich alle Patches anzeigen lassen. Dabei wird auch der Status angezeigt, den das Patch im Hinblick auf den jeweiligen Client aufweist (z.B. unbekannt, anwendbar, nicht anwendbar, installiert, wird installiert). Darüber hinaus haben Sie folgende Ansichtsmöglichkeiten:



Aktualisieren: Hiermit können Sie die Ansicht nach Änderungen aktualisieren und auf den neuesten Stand bringen.

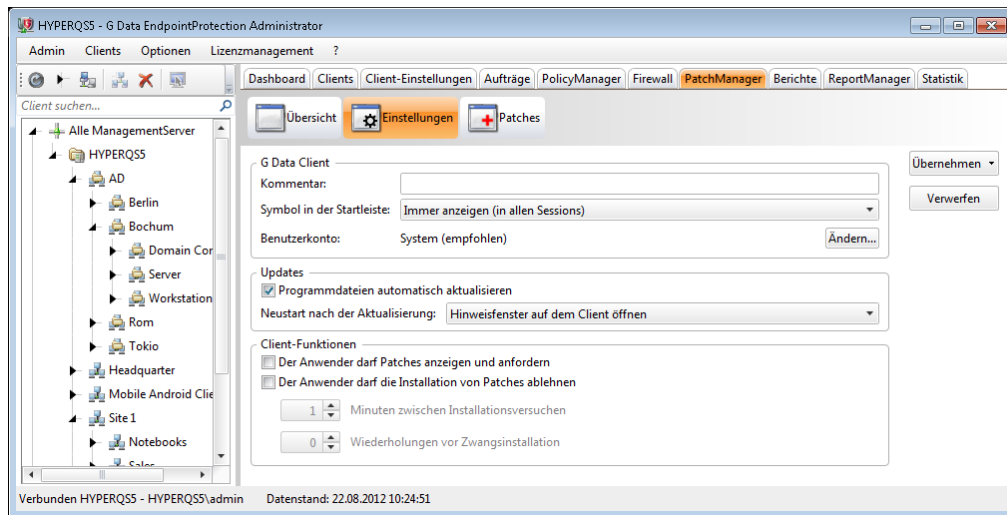


Patches auf der Blacklist ausblenden: Hiermit können Sie in der Übersicht Patches ausblenden, die Sie im Bereich **Patches** auf die Blacklist gesetzt haben.



Nur Patches anzeigen: Hiermit können Sie die Ansicht auf die Patches eingrenzen, die keinen vollständigen Installer haben und so schnell wie möglich auf den Clients eingespielt werden sollten.

Einstellungen



Hier können Sie bestimmen, wie Patches und Updates auf dem Client und den Gruppen eingespielt werden sollen.

G Data Client

Geben Sie hier an, welcher Kommentar beim Einspielen von Patches auf dem Client angezeigt werden soll. Dabei werden - je nach Einstellung - ein Symbol in der Startleiste und der Kommentar auf dem Client eingeblendet.

Updates

Wenn Sie möchten, dass Programmdateien automatisch auf dem Client aktualisiert werden sollen, dann setzen Sie das Häkchen bei Programmdateien automatisch aktualisieren. Sie haben dabei drei Möglichkeiten, den Neustart nach der Programmaktualisierung durchzuführen.

- **Hinweisfenster auf dem Client öffnen:** Der Anwender wird auf dem Client dazu aufgefordert, seinen Computer neu zu starten.
- **Bericht erzeugen:** Es wird ein Bericht erzeugt, der Ihnen als Administrator anzeigt, welche Clients nach der Aktualisierung neu gestartet wurden und wo dies noch nicht der Fall ist.
- **Neustart ohne Abfrage durchführen:** Der Neustart wird erzwungen.

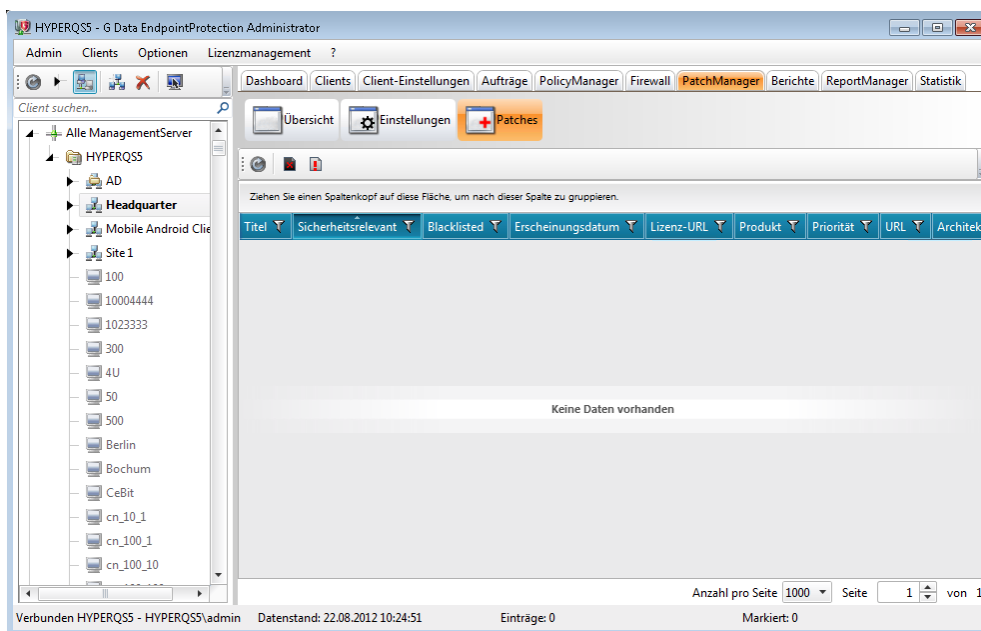
Client-Funktionen

Hier können Sie festlegen, wie viel Ermessensspielraum der Anwender am Client hat.

- **Der Anwender darf Patches anzeigen und anfordern:** Der Anwender kann auf diese Weise aktiv auf benötigte Patches hinweisen.
- **Der Anwender darf die Installation von Patches ablehnen:** Hier können Sie festlegen wie oft und für welchen Zeitraum der Anwender das Installieren von Patches verschieben kann. Prinzipiell ist es dabei nicht möglich, clientseitig das Aufspielen von Patches generell zu unterbinden.

PatchManagement

Im Bereich **Patches** können Sie alle bekannten systemweiten Patches zentral verwalten.

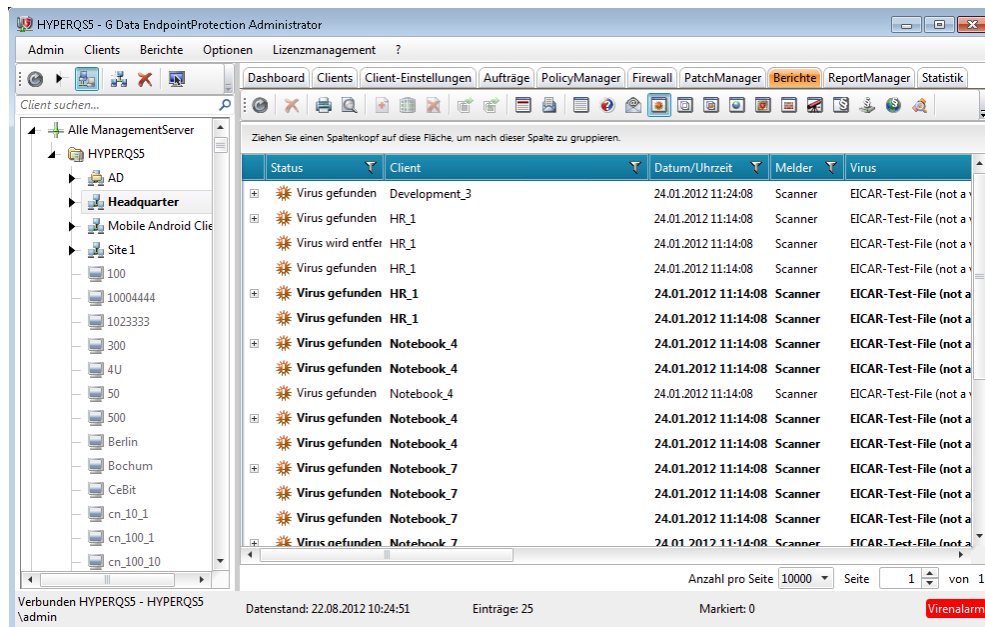


Mit einem rechten Mausklick auf das jeweilige Patch erscheint ein Kontextmenü, indem Sie folgende Möglichkeiten haben:

- **Aktualisieren:** Hier können Sie die Ansicht aktualisieren.
- **Patches auf die Blacklist setzen:** Wenn Sie Patches nicht auf den Clients einspielen möchten, können Sie das jeweilige Patch hier auf die Blacklist setzen. Es wird dann bei der automatischen Aktualisierung nicht berücksichtigt.
- **Patches von der Blacklist entfernen:** Wenn gesperrte Patches doch installiert und verwendet werden sollen, können Sie sie über diese Funktion wieder von der Blacklist entfernen.
- **Patches auf Anwendbarkeit prüfen:**
- **Patches installieren:** Hier können Sie ausgewählte Patches zur Installation auf den Clients freigeben. Je nach Einstellung auf dem Client werden diese dann sofort eingespielt und ein Neustart des Clients erzwungen oder erst später.
- **Eigenschaften:** Hier können Sie sich weitere Informationen zum jeweiligen Patch anzeigen lassen.

Berichte

Alle Virenfunde, Meldungen des PolicyManagers (wenn eine G Data EndpointProtection installiert ist), sowie alle Firewall-Meldungen (bei G Data ClientSecurity oder EndpointProtection) werden in diesem Aufgabenbereich angezeigt. Darüber hinaus werden zusätzlich systemrelevante Meldungen über Installationen, Berichte, Aufforderungen zum Neustart von Clients usw. hier aufgelistet. In der ersten Spalte der Liste wird der Status des Berichtes angezeigt (z.B. **Virus gefunden** oder **Datei in Quarantäne verschoben**). Sie können auf Virenfunde reagieren, indem Sie die Einträge in der Liste wählen und anschließend im Kontextmenü (rechte Maustaste) oder in der Symbolleiste einen Befehl wählen. So lassen sich beispielsweise infizierte Dateien löschen oder in den **Quarantäne-Ordner** verschieben. Im Aufgabenbereich **Berichte** erscheinen alle Berichte unter den von Ihnen vorgegebenen Namen und lassen sich durch einfaches Klicken auf die jeweilige Spaltenbezeichnung nach unterschiedliche Kriterien sortieren. Die Spalte, nach der die aktuelle Sortierung erfolgt, wird dabei durch ein kleines Pfeilsymbol gekennzeichnet.



In der Menüleiste steht Ihnen für den Aufgabenbereich **Berichte** ein zusätzlicher Menüeintrag zur Verfügung. Für die Funktionen, die mit Dateien operieren (löschen, zurückbewegen etc.) müssen Sie in der Berichtsübersicht die jeweilige Datei bzw. Dateien markieren. Folgende Funktionen können Sie hier auswählen.

- **Druckvorlagen:** Hier können Sie spezielle Druckvorlagen vordefinieren, um schnell unterschiedlichste Berichte ausdrucken zu können. Über die Einschränkung der Ausgabedaten, des Berichtszeitraums und das Setzen von Filtern können Sie dabei das Druckvolumen minimieren.
- **Ansicht:** Geben Sie hier an, ob Sie sich alle Berichte, nur Berichte mit nicht entfernten Viren oder nur Quarantäneberichte anzeigen lassen wollen. Sie können sich auch den Inhalt der Quarantäne anzeigen lassen.
- **Abhängige Berichte ausblenden:** Wenn auf Grund verschiedener Aufträge oder mehrfach durchgeführter Aufträge eine Virenmeldung oder ein Bericht doppelt oder mehrfach angezeigt wird, können Sie hiermit die Duplikate ausblenden. Nur der aktuellste Eintrag wird dann angezeigt und kann bearbeitet werden.
- **Gelesene Berichte ausblenden:** Hier können Sie die Berichte ausblenden, die Sie schon gelesen haben.

Wenn Sie die **Scanaufträge** auf Ihrem System so eingestellt haben, dass diese den Virenbefall lediglich protokollieren, können Sie die Virenbekämpfung auch manuell durchführen. Wählen Sie dazu im Bericht eine oder mehrere protokollierte Datei/en aus und führen Sie dann die gewünschte Operation durch:

- **Virus aus der Datei entfernen:** Versucht den Virus aus der Originaldatei zu entfernen.
- **Datei in die Quarantäne verschieben:** Verschiebt die Datei in den **Quarantäne**-Ordner.
- **Datei löschen:** Löscht die Originaldatei auf dem Client.
- **Quarantäne: Säubern und zurückbewegen:** Es wird versucht, den Virus aus der Datei zu entfernen. Wenn dies gelingt, wird die gesäuberte Datei zurück an Ihren Ursprungsort auf dem jeweiligen Client bewegt. Wenn der Virus nicht entfernt werden kann, wird die Datei auch nicht zurückbewegt.
- **Quarantäne: Zurückbewegen:** Verschiebt die Datei aus dem Quarantäne-Ordner zurück auf den Client. **Achtung:** Die Datei wird in ihrem Originalzustand wiederhergestellt und ist weiterhin infiziert.
- **Quarantäne: Zur Internet-Ambulanz senden:** Sollten Sie einen neuen Virus oder ein unbekanntes Phänomen feststellen, senden Sie uns in jedem Fall diese Datei über die Quarantäne-Funktion der G Data Software. Wir analysieren den Virus und werden Ihnen möglichst schnell ein Gegenmittel zur Verfügung stellen. Selbstverständlich behandelt unser **Emergency-AntiViren Service** Ihre eingesandten Daten höchst vertraulich und diskret.
- **Quarantäne: Datei und Bericht löschen:** Löscht die gewählten Berichte. Wenn Berichte gelöscht werden sollen, zu denen eine Quarantäne-Datei gehört, müssen Sie das Löschen noch einmal bestätigen. In diesem Fall werden auch die in Quarantäne befindlichen Dateien gelöscht.

- **Abhängige Berichte löschen:** Wenn auf Grund verschiedener Aufträge oder mehrfach durchgeführter Aufträge eine Virenmeldung oder ein Bericht doppelt oder mehrfach angezeigt wird, können Sie hiermit die doppelten Einträge in der Protokolldatei löschen.

Aktionen und Einstellungen

Folgende Aktionen und Ansichtseinstellungen können Sie in diesem Aufgabenbereich vornehmen:



Aktualisieren: Diese Funktion aktualisiert die Ansicht und lädt die aktuellen **Berichte** vom G Data ManagementServer.



Berichte löschen: Hiermit löschen Sie die ausgewählten Berichte. Wenn Berichte gelöscht werden sollen, zu denen eine **Quarantäne**-Datei gehört, müssen Sie das Löschen noch einmal bestätigen. In diesem Fall werden auch die in Quarantäne befindlichen Dateien gelöscht.



Drucken: Hiermit starten Sie den Druckvorgang für die Berichte. Sie können in dem erscheinenden Auswahlfenster bestimmen, welche Details und Bereiche Sie ausdrucken lassen möchten.



Seitenansicht: Über die Seitenansicht-Funktion können Sie sich vor dem eigentlichen Ausdruck eine Vorschau der zu druckenden Seiten am Monitor ausgeben lassen.



Virus entfernen: Mit dieser Funktion können Sie versuchen, den Virus manuell aus der Originaldatei zu entfernen. Ob dieser Versuch erfolgreich war, wird Ihnen in der Übersicht angezeigt.



In Quarantäne verschieben: Diese Funktion verschiebt die ausgewählten Dateien in den Quarantäne-Ordner. Die Dateien werden verschlüsselt im **Quarantäne**-Ordner auf dem G Data ManagementServer gespeichert. Die Originaldateien werden gelöscht. Durch die Verschlüsselung ist sichergestellt, dass der Virus keinen Schaden anrichten kann. Beachten Sie, dass zu jeder Datei in der Quarantäne ein Bericht gehört. Wenn Sie den Bericht löschen wird auch die Datei im Quarantäne-Ordner gelöscht. Sie können eine Datei aus dem Quarantäne-Ordner zur Untersuchung an den **Emergency-AntiViren Service** senden. Öffnen Sie dazu das Kontextmenü eines Quarantäne-Berichts mit einem Rechtsklick. In dem Berichtdialog klicken Sie dann nach Wahl des Einsendegrunds die Schaltfläche **OK**.



Datei löschen: Mit der Funktion **Datei löschen** löschen Sie die Originaldatei auf dem Client.



Datei aus Quarantäne zurückbewegen: Hiermit verschieben Sie eine Datei aus dem **Quarantäne**-Ordner zurück an den Ursprungsort auf dem Client.

Achtung: Die Datei wird in ihrem Originalzustand wiederhergestellt und ist weiterhin infiziert.



Datei säubern und aus Quarantäne zurückbewegen: Der Virus wird mit dieser Funktion aus der Datei entfernt und die gesäuberte Datei wird auf den Client zurückbewegt. Wenn der Virus nicht entfernt werden kann, verbleibt die Datei im **Quarantäne**-Ordner.



Abhängige Berichte ausblenden: Wenn auf Grund verschiedener Aufträge oder mehrfach durchgeführter Aufträge eine Virenmeldung oder ein Bericht doppelt oder mehrfach angezeigt wird, können Sie hiermit die Duplikate ausblenden. Nur der aktuellste Eintrag wird dann angezeigt und kann bearbeitet werden.



Gelesene Berichte ausblenden



Alle Berichte anzeigen

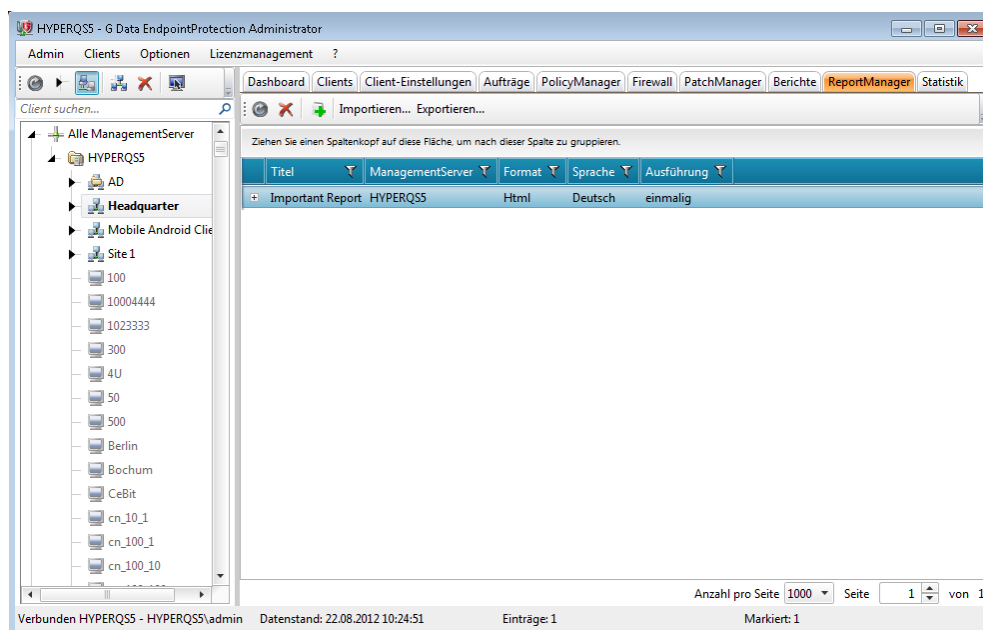


Nur Fehler- und Informationsmeldungen anzeigen

**Nur Mailberichte anzeigen****Alle Berichte mit nicht entfernten Viren anzeigen****Alle Quarantäne-Berichte anzeigen****Inhalt der Quarantäne anzeigen****Alle HTTP-Berichte anzeigen****Nur BankGuard-Berichte anzeigen****Alle Firewall-Berichte anzeigen** (falls Sie eine Softwareversion mit Firewall verwenden)**Nur Berichte der Verhaltensüberwachung anzeigen****Alle Berichte der Anwendungskontrolle anzeigen** (falls Sie eine Softwareversion mit Anwendungskontrolle verwenden)**Alle Berichte der Gerätekontrolle anzeigen** (falls Sie eine Softwareversion mit Gerätekontrolle verwenden)**Alle Berichte der Web-Inhaltskontrolle anzeigen** (falls Sie eine Softwareversion mit Web-Inhaltskontrolle verwenden)**Nur Berichte des Update- / Patch-Managements anzeigen**

ReportManager

Über den ReportManager können Sie zeitplangesteuert Berichte über den Status Ihrer Systemsicherheit konfigurieren und an ausgewählte Empfänger verteilen.



Einstellungs- und Ansichtsoptionen



Aktualisieren: Diese Funktion aktualisiert die Ansicht und lädt die aktuelle Reportliste vom G Data ManagementServer.



Löschen: Die Funktion **Löschen...** löscht alle markierten Reports.



Neue Reportplanung hinzufügen: Hier öffnet sich ein Dialogfenster. Die darin vorhanden Funktionen werden Ihnen im **gleichnamigen Kapitel** erläutert.

Importieren / Exportieren: Hiermit können Sie Einstellungen für den Report importieren und/oder exportieren.

Neue Reportplanung hinzufügen

Hier kann festgelegt werden, welchen Namen der Report haben soll und in welcher Sprache er verfasst werden soll. Unter Empfängergruppen können Sie festlegen, welche Liste von Empfängern diesen Report erhalten soll. Sie können dafür Gruppen verwenden, die Sie unter **Optionen > Server-Einstellungen > E-Mail-Einstellungen** angelegt haben oder hier auch direkt neue Empfängergruppen definieren, darüber hinaus können Sie über das Eingabefeld **Zusätzliche Empfänger** auch weitere E-Mail-Adressen für den jeweiligen Report hinzufügen (Adressaten werden dabei durch Komma getrennt).

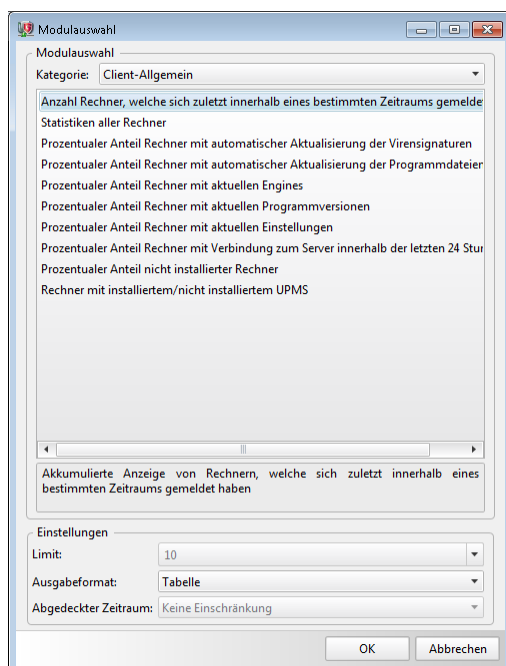
Bei einmaligen Reports können Sie eine Startzeit definieren, bei periodischen Reports können Sie festlegen, wann und in welchem Rhythmus die Benachrichtigung erfolgen soll.

Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** bestimmen, dass nur an Werktagen ein Report durchgeführt wird oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird.

Wird ein **einmaliger Report** angelegt, steht nur die Option **Startzeit verwenden** zur Verfügung. Ohne Angabe einer Startzeit wird der Report sofort nach dem Anlegen gestartet.

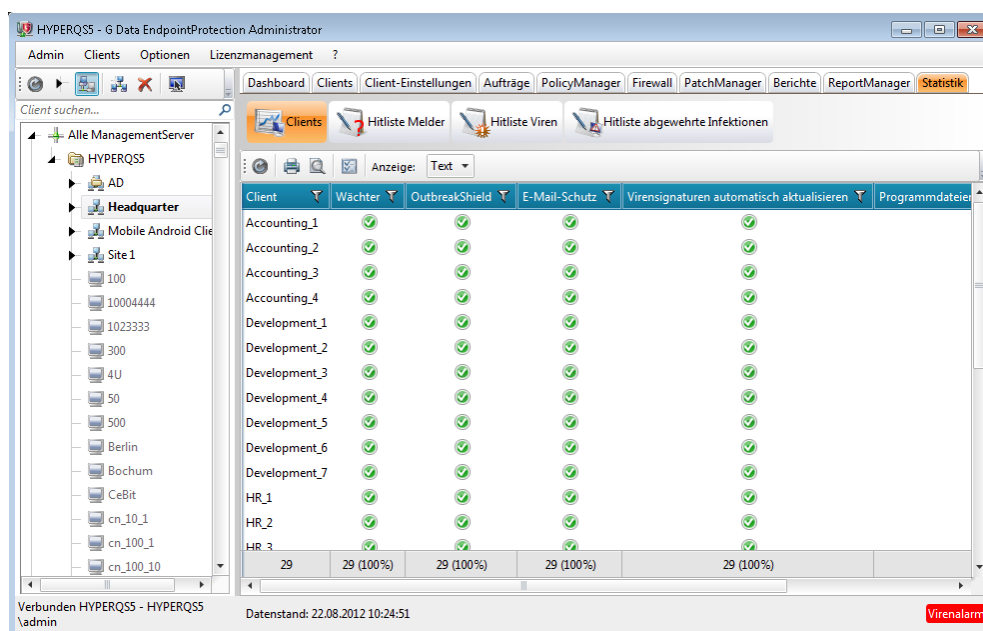
Modulauswahl

Den Inhalt des jeweiligen Reports definieren Sie, indem Sie unter **Ausgewählte Module** auf die Schaltfläche **Neu** klicken und dort eins der auswählbaren Reportmodule aktivieren. Je nach Art des Moduls können Sie aus unterschiedlichen Ausgabeformaten (Tabelle, Line-Chart, Bar-Chart usw.) und Darstellungszeiträumen variieren.



Statistik

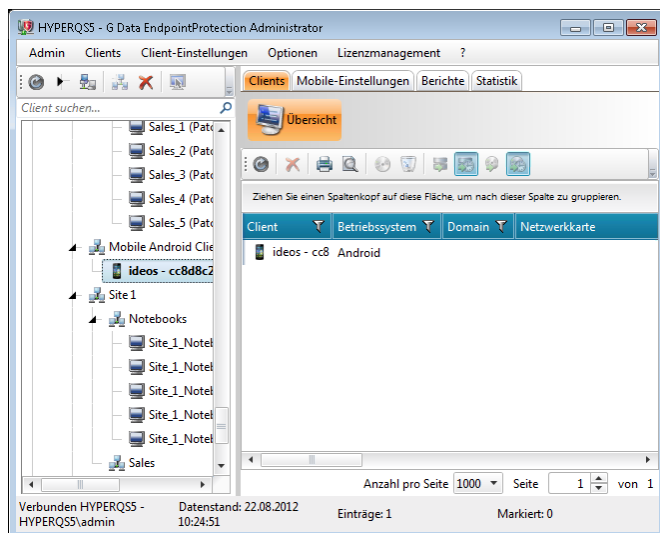
In diesem Aufgabenbereich können Sie sich statistische Informationen zum Virenaufkommen und zu Infektionen auf den Clients anzeigen lassen. Es stehen verschiedene Ansichten zur Verfügung: so kann die Darstellung der Informationen in Textform erfolgen oder auch grafisch aufbereitet werden (Säulen- oder Tortendiagramm). Die entsprechende Ansicht lässt sich unter **Anzeige** auswählen. Es stehen Informationen bereit über den Status der **Clients**, über die **Hitliste der Melder**, die **Hitliste der Viren** und über die **Hitliste der abgewehrten Infektionen**. Wählen Sie den entsprechenden Bereich in der Übersicht aus, um die Informationen einzusehen.



5.4 Mobile Clients

Übersicht

Hier erhalten Sie eine Übersicht über alle verwalteten Mobile Clients und können diese gleichzeitig auch administrieren.



Mit einem rechten Mausklicke auf die Spaltenüberschriften können Sie weitergehende Informationsspalten zum Client zu- oder abwählen.

Zur Administration der Clients und Gruppen stehen Ihnen folgende Schaltflächen zur Verfügung.



Aktualisieren: Diese Funktion aktualisiert die Ansicht und lädt die aktuellen Clienteinstellungen vom G Data ManagementServer.



Löschen: Hiermit entfernen Sie einen Client aus der **Clientübersicht**.



Drucken: Hiermit starten Sie den Druckvorgang für die Client-Übersicht. Sie können in dem erscheinenden Auswahlfenster bestimmen, welche Details und Bereiche der Clients Sie ausdrucken möchten.



Seitenansicht: Hier können Sie vor dem eigentlichen Ausdruck eine Vorschau der zu druckenden Seiten am Monitor ausgeben.



G Data Client installieren: Diese Funktion wird im gleichnamigen Kapitel erläutert.



G Data Client deinstallieren: Diese Funktion wird im gleichnamigen Kapitel erläutert.



Virendatenbank aktualisieren: Aktualisiert die Virendatenbank auf dem Client mit den Dateien vom G Data ManagementServer.



Virendatenbank automatisch aktualisieren: Aktiviert die **automatische Aktualisierung der Virendatenbank**. Die Clients prüfen periodisch, ob aktualisierte Virensignaturen auf dem G Data ManagementServer vorhanden sind und führen die Aktualisierung automatisch durch.



Programmdateien aktualisieren: Aktualisiert die Programmdateien auf dem Client. Es werden die Client-Programmdateien verwendet, die der G Data ManagementServer bereit hält. Nach der Aktualisierung der Programmdateien kann es sein, dass der Client neu gestartet werden muss.



Programmdateien automatisch aktualisieren: Aktiviert die automatische Aktualisierung der Programmdateien. Die Clients prüfen periodisch, ob eine neue Version auf dem G Data ManagementServer existiert und führen die Aktualisierung automatisch durch.

Mobile-Einstellungen

G Data Client

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Kommentar:** Geben Sie hier einen aussagekräftigen Namen für den jeweiligen Client an
- **Gerätename:** Spezifizieren Sie hier anhand der Eingabe des Gerätenamens.

Updates

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Automatisch:** Legen Sie hier fest, ob die Updates der Client-Software für Mobile Devices automatisch oder manuell erfolgen sollen. Falls sie sich für eine automatische Aktualisierung entscheiden, können Sie des Weiteren festlegen, wie oft dies zu erfolgen hat und ob eine Aktualisierung über das Mobilfunknetz oder nur über WLAN erfolgen soll.

Web-Schutz

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Eingeschaltet:** Legen Sie hier fest, ob Mobile Devices beim Zugriff aufs Internet vom G Data Wächter geschützt werden sollen. Dies kann wahlweise als genereller Schutz eingestellt werden oder aber nur, wenn der Zugriff über WLAN erfolgen soll.

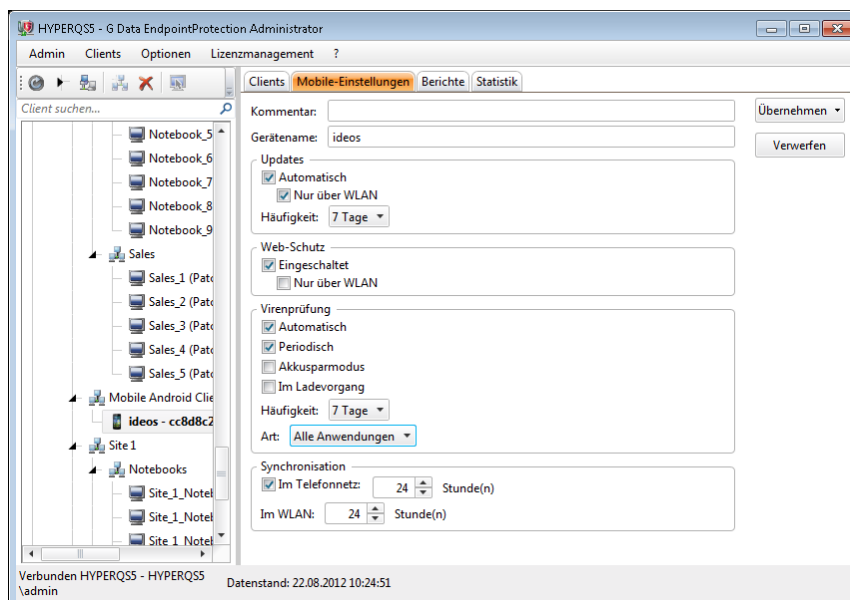
Virenprüfung

Hier haben Sie die Möglichkeit, die Virenprüfung für Mobile Devices an individuelle Gegebenheiten anzupassen:

- **Automatisch:** Die Virenprüfung erfolgt automatisch und muss vom Anwender nicht manuell gestartet werden.
- **Periodisch:** Legen Sie hier fest, wie oft die Virenprüfung zu erfolgen hat, wenn diese automatisch ausgelöst wird. Sie können die Häufigkeit der Prüfung weiter unten einstellen. Hier können Sie außerdem einstellen, ob die Prüfung sich auf alle Anwendungen bezieht oder nur installierte Anwendungen.
- **Akkusparmodus:**
- **Im Ladevorgang:**

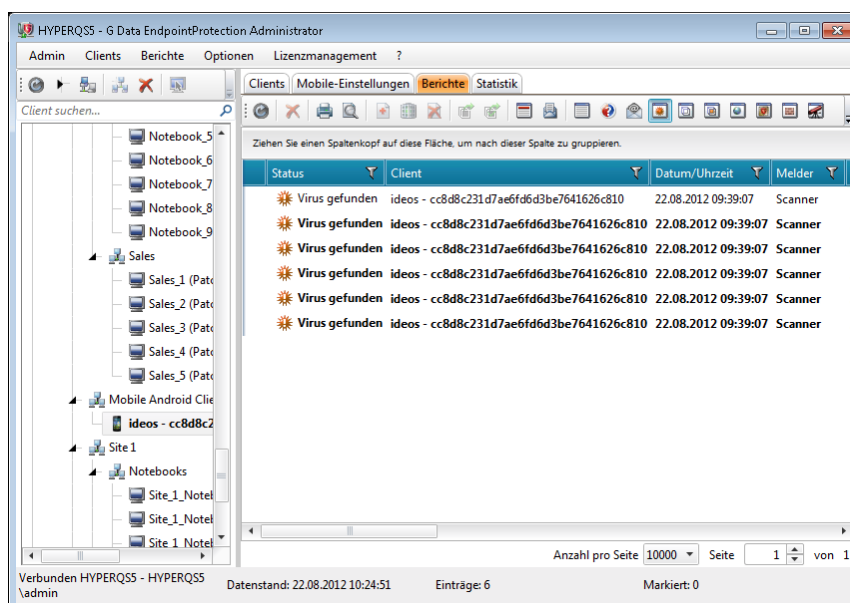
Synchronisation

Hier können Sie festlegen, ob und wie die Virensignaturen auf dem Mobile Device aktualisiert werden sollen. Geben Sie hier den Aktualisierungszyklus in Stunden an und entscheiden Sie, ob eine Synchronisation nur über WLAN oder auch über das Telefonnetz erfolgen soll.



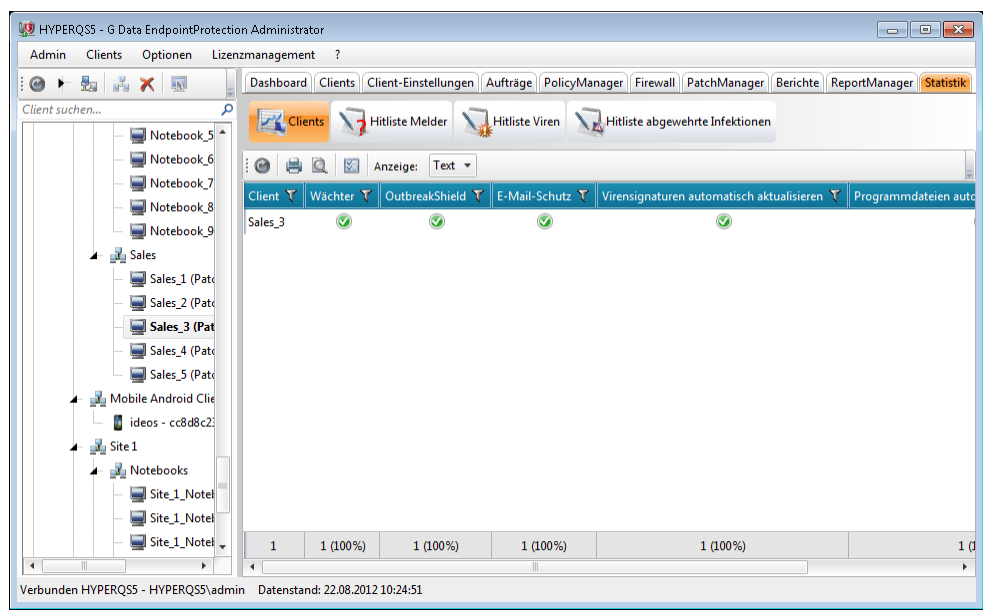
Berichte

Auch für Mobile Devices bietet der G Data Administrator umfangreiche Bericht-Optionen. Da diese weitestgehend identisch mit den Berichten für Clients sind, werden diese auch in folgendem Kapitel **Aufgabenbereiche > Clients > Berichte** beschrieben.



Statistik

Auch für Mobile Devices bietet der G Data Administrator umfangreiche Statistik-Optionen. Da diese weitestgehend identisch mit den Berichten für Clients sind, werden diese auch in folgendem Kapitel **Aufgabenbereiche > Clients > Statistik** beschrieben.



6 G Data Security Client

Die **Client-Software** stellt den Virenschutz für die Clients bereit und führt die ihm vom G Data ManagementServer zugewiesenen Jobs ohne eigene Bedienoberfläche im Hintergrund aus. Die Clients verfügen über eigene Virensignaturen und einen eigenen Scheduler, damit auch im Offline-Betrieb (z.B. bei Notebooks, die keine ständige Verbindung zum G Data ManagementServer haben) Virenanalysen durchgeführt werden können.

6.1 Tray-Icon



Nach der Installation der Client-Software steht dem Benutzer des Clients ein Symbol in der Startleiste zur Verfügung, über den dieser unabhängig von administrativen Vorgaben auch eigenständig sein System auf Virenbefall überprüfen kann. Hierfür ist eine Freigabe dieser Optionen durch den Systemadministrator erforderlich.

Über die rechte Maustaste kann er dabei auf diesem G Data Client-Symbol ein Kontextmenü öffnen, das ihm folgende Optionen anbietet:

Virenprüfung

Über diese Option kann der Anwender gezielt mit dem G Data Security Client seinen Rechner auch außerhalb der im G Data Administrator vorgegebenen Prüfzeiträume auf Viren überprüfen. Der Anwender kann zusätzlich Disketten, CDs/DVDs, den Speicher und Autostart-Bereich, sowie einzelne Dateien oder Verzeichnisse prüfen. Auf diese Weise können auch Notebook-Nutzer, die ihren Rechner nur selten mit dem Firmennetzwerk verbinden, gezielt einen Virenbefall des Systems unterbinden. Außerdem hat er nun die Möglichkeit, virenbefallene Dateien lokal in einen Quarantäne-Ordner zu bewegen, so unschädlich zu machen und zur weiteren Begutachtung dem Netzwerkadministrator bei nächster Gelegenheit zur Verfügung zu stellen.

Der Anwender kann auch aus dem Windows-Explorer heraus Dateien oder Verzeichnisse überprüfen, indem er diese markiert und dann in dem Kontextmenü der rechten Maustaste die Funktion **Auf Viren prüfen (G Data AntiVirus)** verwendet.

Während einer laufenden Virenprüfung wird das Kontextmenü um folgende Einträge erweitert:

- **Priorität Virenprüfung:** Der Anwender hat hier die Möglichkeit, die Priorität der Virenprüfung festzulegen. Bei **Hoch** erfolgt die Virenprüfung schnell, allerdings kann sich das Arbeiten mit anderen Programmen an diesem Rechner deutlich verlangsamen. Bei der Einstellung **Niedrig** dauert die Virenprüfung hingegen vergleichsweise lange, dafür kann währenddessen, ohne größere Einschränkungen, am Client-Rechner weitergearbeitet werden.
- **Virenprüfung anhalten:** Diese Option erlaubt es dem Anwender, eine lokal gestartete Virenprüfung eigenständig anzuhalten. Scanaufträge, die vom G Data ManagementServer festgelegt werden, können nur dann angehalten werden, wenn der Administrator beim Anlegen des Jobs die Option **Anwender kann den Job anhalten oder abbrechen** aktiviert hat.
- **Virenprüfung abbrechen:** Diese Option erlaubt es dem Anwender, eine lokal gestartete Virenprüfung eigenständig abzubrechen. Scanaufträge, die vom G Data ManagementServer festgelegt werden, können nur dann abgebrochen werden, wenn der Administrator beim Anlegen des Jobs die Option **Anwender kann den Job anhalten oder abbrechen** aktiviert hat.
- **Scanfenster anzeigen:** Hiermit kann sich der Anwender das Info-Fenster anzeigen lassen, in dem Verlauf und Fortschritt der Virenprüfung angezeigt werden. Diese Option ist nur verfügbar, wenn eine Virenprüfung lokal gestartet wurde.

Wächter ausschalten

Über diesen Befehl kann der G Data Wächter vom Anwender für einen gewissen Zeitraum (von **5 Minuten** bis **zum nächsten Neustart des Rechners**) ausgeschaltet werden. Dies ist nur dann möglich, wenn er vom Systemadministrator die entsprechenden Rechte erhalten hat. Das zeitweilige Ausschalten des Wächters kann z.B. bei umfangreichen Dateikopiervorgängen sinnvoll sein, da auf diese Weise der Kopiervorgang beschleunigt wird. Der Echtzeit-Virenschutz ist in diesem Zeitraum allerdings ausgeschaltet.

Optionen

Soweit im G Data Administrator die Option **Der Anwender darf E-Mail und Wächteroptionen ändern** aktiviert ist, kann der Anwender auf dem Client die Optionen für die Virenprüfung auf seinem Rechner sowie die Optionen für den im Hintergrund laufenden Wächter an eigene Bedürfnisse anpassen.

Achtung: Auf diese Weise können sämtliche Schutzmechanismen der G Data Software auf dem Client ausgeschaltet werden. Diese Option sollte nur fachlich versierten Anwendern zugänglich sein.

Die sicherheitsrelevanten Einstellungen unter **Optionen...** können auch mit einem Passwort geschützt werden. Dazu vergibt der Administrator für den jeweiligen Client ein individuelles Passwort, mit dem der Anwender die Virenkontrollfunktionen auf dem Client verändern kann. Dieses Passwort wird über den Arbeitsbereich **Einstellungen** im G Data Administrator unter **Passwortschutz für die Änderung von Optionen** vergeben.

Die einzelnen Einstellungsmöglichkeiten, die dem Anwender über den Bereich **Optionen** zur Verfügung stehen, werden ausführlich im Bereich **Programmaufbau des G Data Administrators >**

Aufgabenbereiche > Einstellungen erläutert:

Wenn Sie dem Anwender auf seinem Client die Option **Der Anwender darf selbst Virenprüfungen durchführen** aktivieren, kann dieser unabhängig von den im G Data ManagementServer festgelegten Scanaufträgen seinen Clientrechner auf Viren überprüfen. Die Einstellungen, die für den Anwender auf dem Client hier möglich sind, entsprechen weitestgehend denen, die auch im **Wächter** Verwendung finden.

Quarantäne

Jeder Client hat einen lokalen Quarantäneordner, in den infizierte Dateien (abhängig von den Einstellungen für Wächter / Scanauftrag) verschoben werden können. Eine Datei, die in Quarantäne verschoben wurde, kann, sofern sie einen Virus enthält, keine Schadroutinen ausführen. Infizierte Dateien werden beim Verschieben in die Quarantäne automatisch gepackt und verschlüsselt. Für die Quarantäne bestimmte Dateien, die größer sind als 1 MB werden automatisch immer in der lokalen Quarantäne des Clients abgelegt, um bei einem massiven Virenbefall das Netzwerk nicht unnötig zu belasten. Alle Dateien, die kleiner als 1 MB sind, werden an den Quarantäneordner des G Data ManagementServers übertragen. Diese Einstellungen sind nicht veränderbar. Sollten auf einem mobilen Client ohne Verbindung zum G Data ManagementServer eine infizierte Datei gefunden werden, die kleiner ist als 1 MB, wird sie in der lokalen Quarantäne gespeichert und erst beim nächsten Kontakt zum G Data ManagementServer in die dortige Quarantäne übertragen. Im Quarantäne-Ordner können befallene Dateien desinfiziert werden. Wenn dies nicht funktioniert, lassen sich die Dateien von dort auch löschen und ggf. aus der Quarantäne an ihren Ursprungsort zurückbewegen.

Achtung: Beim Zurückbewegen wird ein Virus nicht entfernt. Sie sollten diese Option nur wählen, wenn das Programm ohne die befallene Datei nicht lauffähig ist und sie diese trotzdem zur Datenrettung benötigen.

Die **Client-Quarantäne** befindet sich im Verzeichnis

%ProgramData% \ G DATA \ AntiVirusKit Client \ Quarantine

Die **G Data ManagementServer-Quarantäne** befindet sich im Verzeichnis

%ProgramData% \ G DATA \ AntiVirus ManagementServer \ Quarantine

Internet-Update

Über den G Data Security Client können auch vom Client-Rechner aus selbstständig Internet-Updates der Virensignaturen durchgeführt werden, falls keine Verbindung zum G Data ManagementServer besteht. Auch diese Option kann vom Netzwerkadministrator für einzelne Clients freigeschaltet werden.

Über die Schaltfläche **Einstellungen und Zeitplanung** kann auch die Aktualisierung der Virensignaturen auf dem Client zeitgesteuert ablaufen.

Firewall

Über den Firewallbereich können Anwender umfangreiche Einstellungen in der Firewall ihres Clients vornehmen, wenn diese Option für den jeweiligen Client serverseitig freigeschaltet wurde. Solange sich der Client im Netzwerk des G Data ManagementServers befindet, wird die Firewall zentral vom Server aus administriert. Die Option **Firewall** steht nur zur Verfügung, wenn im G Data Administrator dem Client die Berechtigung gegeben wurde, die Firewalleinstellungen zu ändern. Für ausführliche Informationen zur Konfiguration und Bedienung der Firewall siehe auch: **Firewall-Einstellungen**.

Info

Über **Info** kann der Versionsstand der installierten G Data Software und der Virensignaturen ermittelt werden.

7 G Data WebAdministrator

Der **G Data WebAdministrator** ist eine webbasierte Steuerungssoftware für den G Data ManagementServer. Mit ihm können Einstellungen für den G Data ManagementServer über ein Webinterface in einem Browser vorgenommen werden.

7.1 Programmaufbau des G Data WebAdministrators

Um den **G Data WebAdministrator** zu nutzen, klicken Sie auf das Desktop-Symbol des G Data WebAdministrators. Nun öffnet sich automatisch Ihr Webbrowser mit einer Anmeldeseite für den Zugang zum G Data WebAdministrator. Geben Sie hier nun wie beim regulären **G Data Administrator** Ihre **Zugangsdaten** ein und klicken Sie dann auf die Schaltfläche **Anmelden**. Der G Data WebAdministrator entspricht in Bedienung und Funktion dem **G Data Administrator**.

8 G Data MailSecurity MailGateway

G Data MailSecurity ist das Softwarepaket zum Komplettschutz Ihrer E-Mail-Kommunikation. Es umfasst:

- **G Data MailSecurity MailGateway:** Das *MailGateway* ist der High-End Virenschutz für Ihre Mail-Korrespondenz und verriegelt so den Haupt-Verbreitungsweg moderner Viren effizient und sicher. Es arbeitet als Gateway unabhängig von Ihrem Mail-Server und ist daher mit beliebiger Mail-Server-Software unter Windows, wie auch Linux kombinierbar.
- **G Data MailSecurity Administrator:** Steuerungssoftware für das Mail-Gateway.

Das Programm ist ein MailGateway für SMTP und POP3 mit integriertem Virenschutz.

- **SMTP:** Eingehende Mails werden nicht mehr an den Mail-Server sondern an das *G Data MailSecurity MailGateway* geschickt. Nach der Virenprüfung werden Sie von dort an den Mail-Server weitergeleitet. *G Data MailSecurity* kann natürlich auch die ausgehenden Mails prüfen. Dazu wird der Mail-Server so konfiguriert, dass er die Mails nicht mehr direkt versendet sondern erst an *G Data MailSecurity* weiterleitet. Das Programm kümmert sich dann um die weitere Verarbeitung.
- **POP3:** Sie können *G Data MailSecurity* auch verwenden, wenn Sie Ihre Mails via POP3 abholen. *G Data MailSecurity* holt die Mails stellvertretend für das anfordernde Programm ab, prüft sie auf Viren und leitet sie dann an das Programm weiter.

Nach Abschluss der Installation steht Ihnen die *MailGateway-Software* zur Verfügung. Neben der eigentlichen Software, die im Hintergrund läuft, wurde automatisch der **Administrator** installiert, über den Sie vollen Zugriff auf die Funktionen und Optionen des MailGateways haben. Diesen Administrator finden Sie bei einer Standardinstallation unter **Start > Programme > G Data MailSecurity > G Data MailSecurity**. Die Einstellungs- und Einflussmöglichkeiten, die Ihnen über den Administrator zur Verfügung stehen, werden in den folgenden Kapiteln ausführlich erläutert.

Sie können das MailGateway auch über jeden anderen Rechner warten, der die Systemvoraussetzungen für das *G Data MailSecurity Administrator-Tool* erfüllt. Wenn Sie das MailGateway also über einen anderen Rechner im Netzwerk ansteuern möchten, installieren Sie dort einfach den Administrator ohne die eigentliche MailGateway-Software. Starten Sie dazu einfach erneut das Setup und wählen die Schaltfläche **G Data MailSecurity Administrator** aus.

Wenn Sie die Administrator-Software beenden, schließen Sie damit nicht das MailGateway. Dieses bleibt weiterhin im Hintergrund aktiv und steuert die Prozesse, die von Ihnen eingestellt wurden.

Der Empfang und Versand von **E-Mails** wird in der Regel über die beiden Protokolle **SMTP** und **POP3** abgewickelt. Dabei dient SMTP (= Simple Mail Transfer Protocol) dazu, Mails an beliebige Empfänger zu verschicken, während POP3 (= Post Office Protocol 3) als übergeordnetes Protokoll dazu verwendet wird, eingegangene Mails in einem speziellen *Postfach* abzulegen, auf welches nur der spezielle Empfänger mittels eines Passwortes Zugriff hat. Je nachdem, wie Ihr Netzwerk aufgebaut ist, kann *G Data MailSecurity* nun an verschiedenen Knotenpunkten greifen, um eingehende Mails auf Virenbefall zu überprüfen:

- Wenn Sie im Netzwerk einen **SMTP-Server** verwenden, kann *G Data MailSecurity* eingehende Mails schon vor dem Erreichen des Mail-Servers überprüfen. Hierzu steht Ihnen die Funktion **Prüfung eingehender Mails (SMTP)** im **Status-Bereich** zur Verfügung.
- Wenn Sie Ihre Mails z.B. über einen aushäusigen Server direkt als **POP3-Mails** bekommen (z.B. über ein **POP3-Sammelkonto**), kann *G Data MailSecurity* auch hier eingreifen, um die POP3-Mails vor dem Öffnen durch den Empfänger auf Virenbefall zu überprüfen. Hierzu steht Ihnen die Funktion **Prüfung eingehender Mails (POP3)** im **Status-Bereich** zur Verfügung.

Selbstverständlich kann *G Data MailSecurity* auch all Ihre ausgehenden Mails vor dem Versand an die Empfänger auf Virenbefall überprüfen. Da für das Versenden von Mails nur das SMTP-Protokoll Verwendung findet, gibt es hier logischerweise keine POP3-Variante. Hier steht Ihnen die Funktion **Prüfung ausgehender Mails (SMTP)** im **Status-Bereich** zur Verfügung.

9 G Data MailSecurity

Administrator

Der *G Data MailSecurity Administrator* ist die Steuerungssoftware für das *G Data MailSecurity MailGateway*, das - vom Systemadministrator zentral gesteuert - den gesamten SMTP- und POP3 basierten E-Mailverkehr mit und in Ihrem gesamten Netzwerk sichert. Der **Administrator** kann passwortgeschützt von jedem Rechner unter Windows gestartet werden. Als ferngesteuerte Jobs sind alle denkbaren Einstellungsänderungen am Virens Scanner und Virensignatur-Updates möglich.

Erster Programmstart



Sie können das **AdministratorTool** zur Steuerung des MailGateways mit einem Klick auf den Eintrag **G Data MailSecurity Administrator** in der Programmgruppe **Start > (Alle) Programme > G Data MailSecurity** des Startmenüs aufrufen. Beim Starten des Administrators werden Sie nach dem Server und dem Kennwort gefragt.

Geben Sie in dem Feld **Server**, den Computernamen oder die IP-Adresse des Computers ein, auf dem das MailGateway installiert wurde. Da Sie jetzt noch kein **Kennwort** vergeben haben, klicken ohne Eingabe eines Kennworts einfach auf die **OK**-Schaltfläche. Es öffnet sich ein Kennworteingabefenster, in dem Sie unter **Neues Kennwort** ein neues Kennwort für den *G Data MailSecurity Administrator* vergeben können.

Sie bestätigen das eingegebenen Kennwort durch erneutes Eintippen im Feld **Neues Kennwort bestätigen** und klicken dann auf **OK**.

Sie können das Kennwort jederzeit im Bereich **Optionen** in der Karteikarte **Erweitert** mit einem Klick auf die Schaltfläche **Kennwort ändern** neu vergeben.

Weitere Programmstarts

Sie können das AdministratorTool zur Steuerung des MailGateways mit einem Klick auf den Eintrag **G Data MailSecurity Administrator** in der Programmgruppe **Start > (Alle) Programme > G Data MailSecurity** des Startmenüs aufrufen. Beim Starten des Administrators werden Sie nach dem Server und dem Kennwort gefragt. Geben Sie in dem Feld **Server**, den Computernamen oder die IP-Adresse des Computers ein, auf dem das MailGateway installiert wurde.

9.1 Programmbereiche

Die Bedienung von *G Data MailSecurity* ist prinzipiell selbsterläuternd und übersichtlich gestaltet. Anhand unterschiedlicher Karteikarten, die Sie über die links im *G Data MailSecurity Administrator* angezeigten Symbole anwählen können, wechseln Sie in den jeweiligen Programmbereich und können dort Aktionen durchführen, Voreinstellungen vornehmen oder Vorgänge überprüfen. Folgende Programmbereiche stehen Ihnen zur Verfügung:



Status



Filter



Wartenschlangen



Aktivität



Virenfunde

Außerdem finden Sie in der oberen Menüleiste der Programmoberfläche übergreifende Funktionen und Einstellungsmöglichkeiten.



Optionen: Hier können Sie grundlegende Einstellungen zum Betrieb Ihrer *G Data MailSecurity* verändern und an individuelle Bedürfnisse anpassen.



Spam-Filter: Über den Spam-Filter haben Sie umfangreiche Einstellungsmöglichkeiten, um Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren.



Update: Im Internet Update-Bereich können Sie grundlegende Einstellungen zum automatischen Download von aktuellen Virensignaturen aus dem Internet vornehmen. Sie können die Zeitplanungen für diese Downloads individuellen Bedürfnissen anpassen und außerdem Updates der Programmdateien von *G Data MailSecurity* durchführen.



Hilfe: Hier rufen Sie die Online-Hilfe zum Produkt auf.



Info: Hier erhalten Sie Informationen zur Programmversion.

Status

Im Status-Bereich des Administrators erhalten Sie grundlegende Informationen zum aktuellen Zustand Ihres Systems und des MailGateways. Diese finden sich rechts vom jeweiligen Eintrag als Text-, Zahl- oder Datumsangabe.



Solange Ihre *G Data MailSecurity* optimal für den Schutz vor Computerviren konfiguriert ist, finden Sie links vor den hier aufgeführten Einträgen ein grünes Ampelsymbol.



Sollte eine Komponente nicht optimal eingestellt sein (z.B. veraltete Virensignaturen, abgeschaltete Virenprüfung), weist Sie ein Achtung-Symbol darauf hin.

Durch doppeltes Anklicken des jeweiligen Eintrags (oder durch Auswählen des Eintrags und Anklicken der **Bearbeiten**-Schaltfläche) können Sie hier direkt Aktionen vornehmen oder in den jeweiligen Programmbereich wechseln. Sobald Sie die Einstellungen einer Komponente mit Achtung-Symbol optimiert haben, wechselt das Symbol im Status-Bereich wieder auf das grüne Ampelsymbol. Folgende Einträge stehen Ihnen zur Verfügung

- **Verarbeitung eingehender Mail:** Die Verarbeitung eingehender Mails sorgt dafür, dass Mails vor der Weitergabe an den Empfänger durch das MailGateway überprüft werden. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen > Eingehend (SMTP)**) und können die Verarbeitung eingehender Mails an individuelle Bedürfnisse anpassen.
- **Virenprüfung eingehender Mail:** Die Prüfung eingehender Mails verhindert, dass infizierte Dateien in Ihr Netz gelangen. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen > Virenprüfung**) und können die Prüfung eingehender Mails an individuelle Bedürfnisse anpassen.
- **Verarbeitung ausgehender Mail:** Die Verarbeitung ausgehender Mails sorgt dafür, dass Mails vor der Weitergabe an den Empfänger durch das MailGateway überprüft werden. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen > Ausgehend (SMTP)**) und können die Verarbeitung eingehender Mails an individuelle Bedürfnisse anpassen.
- **Virenprüfung ausgehender Mail:** Die Prüfung ausgehender Mails verhindert, dass aus Ihrem Netz infizierte Dateien verschickt werden. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen > Virenprüfung**) und können die Prüfung ausgehender Mails an individuelle Bedürfnisse anpassen.

- **OutbreakShield:** Mit dem **OutbreakShield** können Schädlinge in Massenmails schon erkannt und bekämpft werden, bevor aktualisierte Signaturen dafür verfügbar sind. Das OutbreakShield erfragt dabei über das Internet besondere Häufungen von verdächtigen Mails und schließt dabei quasi in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Signaturen besteht.
- **Automatische Updates:** Die Virensignaturen können selbstständig aktualisiert werden. Sie sollten die Option für automatische **Updates** generell aktiviert haben. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Internet Update**) und können die Updatefrequenz an individuelle Bedürfnisse anpassen.
- **Datum der Virensignaturen:** Je aktueller die Virensignaturen, desto sicherer ist Ihr Virenschutz. Sie sollten die **Virensignaturen** so oft wie möglich updaten und diesen Prozess möglichst automatisieren. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Internet Update**) und können auch direkt ein Internet Update (unabhängig von etwaigen Zeitplänen) durchführen.
- **Spam-Filter:** Über den **Spam-Filter** haben Sie umfangreiche Einstellungsmöglichkeiten, um Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren.
- **Spam-OutbreakShield:** Mit dem **Spam-OutbreakShield** können Massenmails schnell und sicher erkannt und bekämpft werden. Das Spam-OutbreakShield erfragt dabei vor dem Abruf von Mails über das Internet besondere Häufungen von verdächtigen Mails ab und lässt diese gar nicht erst in das Postfach des Empfängers gelangen.

Wenn Sie bei der Installation die Option **E-Mail-Statistik** aktiviert haben, können Sie über die Schaltfläche **Statistik** Zugriff auf die statistische Auswertung Ihres Mailverkehrs bzw. Spamaufkommens nehmen. Das Konfigurieren der Statistik erfolgt dabei im **Optionen**-Menü des Administrators auf der Registerkarte namens **Datenbank**.

Filter

Im Filter-Bereich können Sie auf komfortable Weise Filter nutzen, die ein- und ausgehende Mails blocken oder automatisch möglicherweise gefährlichen Inhalte aus Mails entfernen. Die jeweiligen Filter werden in der Liste im Filter-Bereich angezeigt und können über die Häkchenfelder links vom jeweiligen Eintrag beliebig an- bzw. abgeschaltet werden.

Wenn sich ein Häkchen im Häkchenfeld befindet, ist der jeweilige Filter aktiv. Wenn sich kein Häkchen im Häkchenfeld befindet, ist der Filter nicht aktiv.

- **Import:** Sie können einzelne Filter mit ihren speziellen Einstellungen auch als XML-Datei speichern und ggf. erneut oder auf anderen Rechnern nutzen.
- **Export:** Sie können einzelne Filter mit ihren speziellen Einstellungen auch als XML-Datei speichern und ggf. erneut oder auf anderen Rechnern nutzen. Um mehrere Filter zu exportieren, wählen Sie diese bitte mit der Maus aus und halten dabei die **Strg-Taste** gedrückt.
- **Neu:** Über die **Neu**-Schaltfläche können Sie neue Filterregeln anlegen. Wenn Sie einen neuen Filter anlegen, öffnet sich ein Auswahlfenster, in dem Sie den grundlegenden Filtertyp festlegen können. Alle weiteren Angaben zum zu erstellenden Filter können Sie dann in einem dem Filtertyp angepassten Assistentenfenster angeben. Auf diese Weise erstellen Sie auf sehr komfortable Weise Filter gegen jede erdenkliche Gefährdung.
- **Bearbeiten:** Über die **Bearbeiten**-Schaltfläche können Sie vorhandene Filter bearbeiten.
- **Löschen:** Um einen Filter endgültig zu löschen, markieren Sie diesen bitte mit einem einfachen Mausklick und verwenden dann die **Löschen**-Schaltfläche.
- **Statistik:** Zu jedem Filter können Sie statistische Informationen aufrufen.
- **Protokoll:** Für den **Spam-Filter** gibt es ein Protokoll mit einer Liste, in der die als Spam eingestufteten Mails aufgelistet sind. Dem Protokoll kann man auch entnehmen, welche Kriterien für die Einstufung als Spam verantwortlich waren (Spam-Index-Werte). Hier können Sie ggf. bei einer fälschlichen Einstufung einer Mail als Spam den OutbreakShield-Server online darüber informieren, dass hier eine Fehlkenntung (*False Positive*) vorliegt. Die Mail wird dann vom OutbreakShield erneut geprüft und - falls sie tatsächlich fälschlicherweise als Spam erkannt wurde - des Weiteren als unbedenklich eingestuft.
Achtung: Hierbei wird lediglich eine Prüfsumme übermittelt und nicht der Inhalt dieser Mail.

Selbstverständlich ist Ihr Netzwerk auch unabhängig von individuellen Filterregeln vor Virenbefall geschützt, da *G Data MailSecurity* ständig im Hintergrund eingehende und ausgehende Mails überprüft. Filterregeln dienen eher dazu, Ihre E-Mail-Accounts vor unerwünschten Mails, Spam und unsicheren Skripten zu bewahren und potentielle Virenherde schon vor der eigentlichen Virenerkennung durch *G Data MailSecurity* zu minimieren.

Allgemeine Filterfunktionen

Generell können Sie bei allen Filtertypen unter **Name** einen aussagekräftigen Namen für den jeweiligen Filter angeben, mit dem dieser Filter dann in der Liste des Filter-Bereichs angezeigt wird und Sie können unter **Bemerkung** interne Bemerkungen und Notizen zu dem betreffenden Filter angeben. Unter **Richtung** können Sie generell bestimmen, ob eine Filterregel nur für **eingehende Mails**, nur für **ausgehende Mails** oder beide Richtungen gelten soll.

Reaktion

Im Abschnitt **Reaktion** können Sie festlegen, wie mit Mails verfahren werden soll, sobald Sie die Filterkriterien erfüllen, also als Spam-Mails definiert wurden.

Sie können dabei den Text für die Funktionen **Absender benachrichtigen** und **Meldung an folgende Personen senden** individuell gestalten.

Klicken Sie dazu einfach auf die Schaltfläche rechts von der jeweiligen Reaktion. Dabei können Sie auch Platzhalter verwenden, die entsprechende Angaben zur zurückgewiesenen Mail in den Benachrichtigungstext übernehmen. Im frei definierbaren Text für den **Betreff** und den **Mailtext** stehen Ihnen folgende **Platzhalter** (definiert durch ein Prozentzeichen mit einem anschließenden Kleinbuchstaben) zur Verfügung:

%s	Absender
%r	Empfänger
%c	Cc
%d	Datum
%u	Betreff
%h	Header
%i	Absender-IP

Die unterschiedlichen Filtertypen werden in den folgenden Abschnitten ausführlich erläutert:

Lesebestätigung filtern

Dieser Filter löscht Anforderungen für eine Lesebestätigung. Dabei handelt es sich um eine Rückantwortmail, die automatisch abgeschickt wird, sobald der Empfänger eine solche Mail mit Lesebestätigung gelesen hat.

HTML-Skripte deaktivieren

Dieser Filter deaktiviert Skripte im HTML-Teil einer Mail. Skripte, die in einer Internetseite durchaus einen Sinn haben mögen, sind - wenn sie in eine HTML-Mail eingebunden sind - eher störend. In manchen Fällen werden HTML-Skripte auch aktiv dazu verwendet, Rechner zu infizieren, wobei Skripte die Möglichkeit haben, sich nicht erst durch das Öffnen einer infizierten Anlage weiterzuverbreiten, sondern alleine schon in der **Vorschauansicht einer Mail** wirksam werden können.

Externe Referenzen deaktivieren

Viele Newsletter und Produktinformationen im **HTML-Mailformat** beinhalten Links, die erst dann ausgeführt und angezeigt werden, wenn die Mail geöffnet wird. Dies können z.B. Grafiken sein, die nicht mit der Mail versandt wurden, sondern erst über einen **Hyperlink** automatisch nachgeladen werden. Da es sich hierbei nicht nur um *harmlose* Grafiken handeln kann, sondern durchaus auch um Schadroutinen, ist es sinnvoll, diese Referenzen zu deaktivieren. Der eigentliche Mail-Text ist von dieser Deaktivierung nicht betroffen.

Greylist-Filter

Greylist-Filter sind eine effektive Methode, um das Spam-Aufkommen zu reduzieren. Hierbei werden E-Mails von unbekannten Absendern nicht sofort beim ersten Zustellversuch über den SMTP-Server an den Mail-Empfänger übermittelt. Da Spam-Versender in der Regel keine Queue-Verwaltung nutzen und ihre Mails selten ein zweites Mal an denselben SMTP-Server schicken, kann die Anzahl an übermittelten Spam-Mails erheblich sinken.

- **Wartezeiten (Minuten):** Über diese Einstellungen können Sie festlegen, wie lange die Übermittlung verdächtiger Mails blockiert werden soll. Nach Ablauf dieser Zeitspanne wird die Mail bei einem erneuten Sendeversuch dann übermittelt. Wenn der Adressat auf diesen Absender reagiert, wird dieser aus dem Greylist-Filter herausgenommen und in eine Whitelist eingetragen. Nun wird die Zustellung dieser Mails nicht mehr blockiert bzw. verzögert.
- **Lebenszeiten (Tage):** Damit die Whitelist der erwünschten Absender aktuell bleibt, verbleibt eine Absenderadresse nur eine bestimmte Zeit auf der Whitelist, bevor sie wieder auf Greylist-Status gesetzt wird. Der Timer wird für den jeweiligen Absender bei jedem neuen Mailversand wieder zurückgesetzt. Wenn Sie hier z.B. einen Wert über 30 Tage eintragen, können Sie auch erwünschte monatliche Newsletter permanent auf der Whitelist führen.

Der Greylist-Filter kann nur dann ausgewählt werden, wenn auch der **Spam-Filter** von *G Data MailSecurity* aktiviert ist. Außerdem muss eine SQL-Datenbank auf dem Server installiert sein.

Anhänge filtern

Beim Filtern von Anhängen haben Sie eine große Auswahl von Möglichkeiten, um **Mail-Anhänge** (= **Attachments**) und Anlagen zu filtern. Die meisten E-Mailviren verbreiten sich über solche Attachments, die in den meisten Fällen mehr oder minder gut verborgene ausführbare Dateien enthalten. Dabei kann es sich um eine klassische EXE-Datei handeln, die ein Schadprogramm enthält, aber auch um VB-Skripte, die sich unter bestimmten Voraussetzungen sogar hinter vermeintlich sicheren Grafik-, Film- oder Musikdateien verbergen. Generell sollte jeder Anwender bei der Ausführung von Mail-Anhängen große Vorsicht walten lassen und im Zweifelsfall lieber noch einmal eine Rückfrage beim Absender einer Mail durchführen, bevor er eine Datei ausführt, die er nicht ausdrücklich angefordert hat. Unter **Dateierweiterungen** können Sie die Dateierweiterungen aufzählen, auf die Sie den jeweiligen Filter anwenden möchten. Dabei können Sie z.B. alle ausführbaren Dateien (z.B. EXE und COM-Dateien) in einem Filter zusammenfassen, aber auch andere Formate (z.B. MPEG, AVI, MP3, JPEG, JPG, GIF etc.) filtern, wenn diese aufgrund Ihrer Größe eine Belastung für den Mail-Server darstellen. Selbstverständlich können Sie auch beliebige **Archivdateien** (z.B. ZIP, RAR oder CAB) filtern. Trennen Sie bitte alle Dateierweiterungen einer Filtergruppe durch Semikolon, z.B. *.exe; *.dll.

Geben Sie unter **Modus** an, ob Sie die unter **Dateierweiterungen** aufgelisteten Dateierweiterungen erlauben möchten (**Nur angegebene Anhänge erlauben**) oder verbieten (**Angegebene Anhänge filtern**).

Über die Funktion **Auch Anhänge in eingebetteten Mails filtern** sorgen Sie dafür, dass die Filterung der unter **Dateierweiterungen** ausgewählten Anlagentypen auch in Mails stattfindet, die selber eine Anlage einer Mail darstellen. Diese Option sollte generell aktiviert sein.

Über **Anhänge nur umbenennen** werden die zu filternden Anlagen nicht automatisch gelöscht, sondern nur umbenannt. Dies ist z.B. bei ausführbaren Dateien (wie z.B. EXE und COM) durchaus sinnvoll, aber auch bei Microsoft Office-Dateien, die möglicherweise ausführbare Skripte und Makros enthalten könnten. Durch das Umbenennen einer Anlage kann Sie nicht unbedacht durch einfachen Mausklick geöffnet werden, sondern muss vom Empfänger erst abgespeichert und ggf. wieder umbenannt werden, bevor er sie verwenden kann. Wenn das Häkchen bei **Anhänge nur umbenennen** nicht gesetzt ist, werden die entsprechenden Anhänge direkt gelöscht.

Unter **Suffix** geben Sie die Zeichenfolge ein, mit der Sie die eigentliche Dateiendung erweitern möchten, auf diese Weise wird die Ausführbarkeit einer Datei durch einfaches Anklicken verhindert (z.B. *.exe_danger).

Unter **Meldung im Text der Mail einfügen** können Sie den Empfänger der gefilterten Mail darüber informieren, dass ein Anhang aufgrund einer Filterregel gelöscht oder umbenannt wurde.

Inhaltsfilter

Über den Inhaltsfilter können Sie E-Mails, die bestimmte Themen oder Texte enthalten auf bequeme Weise blocken. Geben Sie dazu unter **Regulärer Ausdruck** einfach die Schlüsselwörter und Ausdrücke ein, auf die *G Data MailSecurity* reagieren soll und geben Sie unter **Suchbereich** an, in welchen Bereichen einer Mail nach diesen Ausdrücken gesucht werden soll. Über die **Neu**-Schaltfläche rechts vom Eingabefeld für **Regulärer Ausdruck** können Sie auf bequeme Weise Text eingeben, der eine Filteraktion hervorruft. Dabei können Sie Text auf beliebige Weise mit den logischen Operatoren **UND** und **ODER** verknüpfen.

Wenn Sie z.B. *Alkohol UND Drogen* eingeben, würde der Filter bei einer Mail, die z.B. die Begriffe *Alkohol* und *Drogen* enthält, aktiviert werden, nicht aber bei einer Mail, die nur den Begriff *Alkohol* oder nur den Begriff *Drogen* enthält. Der logische Operator **UND** setzt also voraus, dass alle mit **UND** verknüpften Elemente vorhanden sind, der logische Operator **ODER** setzt lediglich voraus, dass ein Element vorhanden ist.

Sie können auch ohne die Eingabehilfe unter **Regulärer Ausdruck** beliebige Suchbegriffe miteinander kombinieren. Geben Sie dazu einfach die **Suchbegriffe** ein und verknüpfen diese mit den logischen Operatoren:

ODER	entspricht dem Trennstrich	(AltGr + <)	
UND	entspricht dem Kaufmanns- Und	(Shift + 6)	&

Absenderfilter

Über den Absenderfilter können Sie E-Mails, die von bestimmten Absendern kommen, auf bequeme Weise blocken. Geben Sie dazu unter **Adressen/Domains** einfach die E-Mail-Adressen oder Domain-Namen ein, auf die *G Data MailSecurity* reagieren soll. Mehrere Einträge können Sie durch Semikolon voneinander trennen.

Sie können auch Mails ohne Absenderangabe automatisch ausfiltern.

Empfängerfilter

Über den Empfängerfilter können Sie E-Mails für bestimmte Empfänger auf bequeme Weise blocken. Geben Sie dazu unter **Adressen/Domains** einfach die E-Mail-Adressen oder Domain-Namen ein, auf die *G Data MailSecurity* reagieren soll. Mehrere Einträge können Sie durch Semikolon voneinander trennen.

Sie können auch Mails mit leerem Empfängerfeld (also Mails, die nur Bcc- und/oder Cc-Empfänger enthalten) automatisch ausfiltern.

Spam filtern

Über den Spam-Filter haben Sie umfangreiche Einstellungsmöglichkeiten, um Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren. Das Programm prüft viele Merkmale der Mails, die typisch für Spam sind. Anhand der zutreffenden Merkmale wird ein Wert errechnet, der die Wahrscheinlichkeit für Spam widerspiegelt. Dazu stehen Ihnen mehrere Karteikarten zur Verfügung, in denen Ihnen alle relevanten Einstellungsmöglichkeiten thematisch gegliedert zur Verfügung stehen. Die Funktionsweise und Einstellungsmöglichkeiten des Spam-Filters werden im Kapitel **Spam-Filter** ausführlich erläutert.

IP-Filter

Der IP-Filter unterbindet den Empfang von Mails, die von bestimmten Servern abgesendet werden. Geben Sie hier unter **Name** und **Bemerkung** Informationen dazu ein, wieso sie die jeweiligen IP-Adressen sperren möchten und dann jede einzelne IP-Adresse unter **Von folgenden IP-Adressen keine Mails annehmen** ein. Klicken Sie auf **Hinzufügen** und die aktuell eingetragene IP-Adresse wird in die Liste der gesperrten IP-Adressen übernommen.

Unter **Modus** können Sie dabei festlegen, ob der IP-Filter im Whitelist-Modus nur bestimmte IP-Adressräume erlauben soll oder im Blacklist-Modus nur bestimmte IP-Adressräume sperren soll.

[Sie können die Liste der IP-Adressen auch als txt-Datei exportieren oder eine entsprechende txt-Liste mit IP-Adressen importieren.](#)

Sprachenfilter

Mit dem Sprachenfilter können Sie automatisch Mails bestimmter Landessprachen als Spam definieren. Wenn Sie also in der Regel z.B. keinen Mailkontakt zu englischsprachigen Personen haben, können Sie über die Definierung von *Englisch* als Spam-Sprache sehr viele Spams ausfiltern. Wählen Sie hier einfach die Sprachen aus, bei denen Sie davon ausgehen, dass Sie in eben diesen Sprachen keine regulären Mails erhalten und *G Data MailSecurity* erhöht damit die Spameinschätzung für diese Mails erheblich.

Warteschlangen

Im Warteschlangen-Bereich haben Sie jederzeit Überblick über eingehende und ausgehende Mails, die im MailGateway auflaufen und auf Viren und/oder Content überprüft werden. Die Mails werden in der Regel sofort weitergeleitet, durch das MailGateway nur minimal verzögert und dann auch sofort wieder aus der Warteschlangenliste gelöscht. Sobald eine Mail nicht zustellbar ist oder sich Verzögerungen in der Zustellung ergeben (weil der jeweilige Server z.B. momentan nicht erreichbar ist), erfolgt in der Warteschlangenliste ein entsprechender Eintrag. *G Data MailSecurity* versucht dann in einstellbaren Abständen (unter **Optionen > Warteschlange**) die Mail erneut zu verschicken. Eine nicht erfolgte oder verzögerte Mailzustellung wird auf diese Weise jederzeit dokumentiert. Über die Schaltfläche **Eingehend/Ausgehend** wechseln Sie von der **Listenansicht für eingehende Mails** zur **Listenansicht für ausgehende Mails**. Über die Schaltfläche **Jetzt wiederholen** können Sie eine markierte Mail, die nicht zugestellt werden konnte - unabhängig von den Zeitvorgaben, die Sie für eine erneute Zustellung unter **Optionen > Warteschlange** definiert haben - erneut zustellen. Mit der **Löschen**-Schaltfläche entfernen Sie eine nicht zustellbare Mail endgültig aus der Queue.

Aktivität

Im Aktivität-Bereich haben Sie jederzeit Überblick über die von *G Data MailSecurity* durchgeführten Aktionen. Diese werden mit **Uhrzeit**, **ID** und **Aktionsbeschreibung** in der Aktivität-Liste aufgelistet. Mit dem Scrollbalken rechts können Sie in dem Protokoll auf und abscrollen. Über die **Zurücksetzen**-Schaltfläche löschen Sie das bis dahin erzeugte Protokoll und *G Data MailSecurity* beginnt die Aufzeichnung der Aktivitäten erneut. Mit der Funktion **Bildlauf deaktivieren** wird die Liste weiterhin aktualisiert, aber die neuesten Aktivitäten werden nicht direkt an erster Stelle eingeblendet. Sie können dann konzentrierter in der Liste scrollen.

[Über die **ID** können Sie die protokollierten Aktionen eindeutig einzelnen Mails zuordnen. So gehören Vorgänge mit gleicher ID immer zusammen \(z.B. 12345 Lade Mail, 12345 Verarbeite Mail, 12345 Sende Mail\).](#)

Virenfunde

Im Virenfunde-Bereich werden Sie detailliert darüber informiert, wann *G Data MailSecurity* eine infizierte Mail ermittelt hat, welche Maßnahmen dahingehend erfolgten, um welche Art von Virus es sich handelt und wer die eigentlichen Sender und Empfänger dieser betreffenden Mail sind. Über **Löschen** entfernen Sie die jeweils ausgewählte Virenmeldung aus der Virenfunde-Liste.

9.2 Menüleiste

Hier finden Sie übergeordnete Funktionen der Administrationssoftware.

Optionen

Im Optionen-Bereich können Sie umfangreiche Einstellungen vornehmen, um *G Data MailSecurity* optimal auf die Gegebenheiten anzupassen, die in Ihrem Netzwerk existieren. Dazu stehen Ihnen verschiedene thematisch untergliederte Einstellungsbereiche in verschiedenen Karteikarten zur Verfügung, die Sie durch Anklicken des jeweiligen Karteireiters in den Vordergrund holen.

Eingehend (SMTP)

In diesem Bereich haben Sie die Möglichkeit, alle notwendigen Einstellungen zur Virenkontrolle eingehender **SMTP-Mails** auf Ihrem Mail-Server vorzunehmen.

Empfang

Hier können Sie festlegen, ob **eingehende Mails** verarbeitet werden sollen. Generell ist hier **Port 25** voreingestellt. Sollte auf Grund besonderer Umstände dieser **Standardport** nicht verwendet werden, können Sie über die Schaltfläche **Konfigurieren** auch andere Port-Einstellungen und Protokoll-Einstellungen für eingehende Mails definieren.

Weiterleitung

Zur **Weiterleitung** der eingehenden Mails an Ihren Mail-Server deaktivieren Sie bitte die Option **DNS zum Versenden der Mails verwenden** und geben Sie unter **Mails an diesen SMTP-Server weiterleiten** den gewünschten Server an. Geben Sie bitte auch den **Port** an, über den die Mails an den SMTP-Server weitergeleitet werden sollen. Sollten mehrere Netzwerkkarten zur Verfügung stehen, können Sie über die Auswahl unter **Absende-IP** festlegen, welche dieser Karten Sie verwenden möchten.

Schutz vor Relaying

Um einen Missbrauch Ihres Mail-Servers zu unterbinden, können und sollten Sie unter **Eingehende Mails nur für folgende Domains akzeptieren** die Domains festlegen, an die SMTP-Mails versendet werden dürfen. Auf diese Weise kann Ihr Server nicht zur Weiterleitung von SPAM-Mails an andere Domains missbraucht werden.

Achtung: Wenn Sie hier keine Domains eintragen, werden auch keine Mails angenommen. Sollen alle Mails von allen Domains angenommen werden, muss hier ein ***.*** (Sternchen Punkt Sternchen) hinzugefügt werden.

Der **Relay-Schutz** kann wahlweise auch über eine Liste von gültigen E-Mail-Adressen realisiert werden. Mails für Empfänger, die nicht auf der Liste stehen, werden nicht angenommen. Um die Pflege dieser Mailadressen zu automatisieren, können diese automatisch und periodisch aus dem ActiveDirectory gelesen werden. Für die **ActiveDirectory-Anbindung** wird mindestens das **.Net-Framework 1.1** benötigt.

ActiveDirectory ist eine in Microsoft Windows verwendete Datenbank, in der vom Administrator Informationen zu Objekten (z.B. Diensten, Ressourcen oder Benutzern) im Netzwerk zentral organisiert, bereitgestellt und überwacht werden können.

Ausgehend (SMTP)

In diesem Bereich haben Sie die Möglichkeit, alle notwendigen Einstellungen zur Virenkontrolle ausgehender **SMTP-Mails** auf Ihrem Mail-Server vorzunehmen.

Empfang

Über das Häkchenfeld **Ausgehende Mail verarbeiten** legen Sie fest, ob Sie ausgehende SMTP-Mails auf Virenbefall kontrollieren möchten oder nicht. Unter **IP-Adressen/Subnetze der Rechner, die ausgehende Mails senden** können Sie bestimmen, von welchen IP-Adressen die zu überprüfenden Mails kommen. Wenn mehrere IP-Adressen dafür in Frage kommen, trennen Sie bitte die einzelnen IP-Adressen durch ein Komma voneinander ab. Diese Eingabe ist nötig, damit das MailGateway eingehende und ausgehende Mails voneinander unterscheiden kann. Generell ist der **Port 25** für den Empfang ausgehender Mails voreingestellt. Sollte auf Grund besonderer Umstände dieser Standardport nicht verwendet werden, können Sie über die Schaltfläche **Konfigurieren** auch andere Einstellungen für eingehende Mails definieren.

Weiterleitung

Aktivieren Sie den Eintrag **DNS zum Versenden der Mails verwenden**, damit die Mails direkt an den für die Zieldomäne zuständigen Mail-Server geschickt werden. Wenn Sie die Mails indirekt über ein **Relay** (z.B. einen Provider) versenden möchten, deaktivieren Sie **DNS zum Versenden der Mails verwenden** und geben Sie unter **Mails an diesen SMTP-Server weiterleiten** das Relay an. Sollten mehrere **Netzwerkarten** zur Verfügung stehen, können Sie über die Auswahl unter **Absende-IP** festlegen, welche dieser Karten Sie verwenden möchten.

Eingehend (POP3)

In diesem Bereich haben Sie die Möglichkeit, alle notwendigen Einstellungen zur Virenkontrolle eingehender **POP3-Mails** auf Ihrem Mail-Server vorzunehmen.

Anfragen

Unter **POP3-Anfragen verarbeiten** aktivieren Sie die Möglichkeit, über *G Data MailSecurity* Ihre **POP3-Mails** vom entsprechenden POP3-Server abzuholen, auf Viren zu überprüfen und über Ihren Mail-Server an die Empfänger weiterzuleiten. Sie müssen dazu gegebenenfalls den **Port** angeben, den Ihr Mailprogramm für POP3-Anfragen verwendet (in der Regel **Port 110**). Mit der Funktion **Zeitüberschreitung beim Mail-Programm vermeiden** überbrücken Sie die Zeit, die *G Data MailSecurity* zum Überprüfen der E-Mails benötigt und verhindern so, dass der Empfänger beim Abruf seiner POP3-Mails möglicherweise vom Mail-Programm einen **TimeOut-Fehler** erhält, weil die Daten nicht sofort zur Verfügung stehen (sondern je nach Mail-Aufkommen erst ein paar Sekunden verzögert).

POP3-basierte Mailprogramme können **manuell konfiguriert** werden. Verwenden Sie dabei in Ihrem Mail-Programm **127.0.0.1** bzw. den Server Ihres MailGateways als eingehenden POP3-Server und schreiben Sie den Namen des externen Mail-Servers, mit einem Doppelpunkt getrennt, vor den Benutzernamen. Also z.B. statt *POP3-Server:mail.xxx.de/Benutzername:Erika Musterfrau* schreiben Sie *POP3-Server:127.0.0.1/Benutzername:mail.xxx.de:Erika Musterfrau*. Um eine manuelle Konfiguration durchzuführen, informieren Sie sich bitte auch in der Bedienungsanleitung Ihres Mail-Programms über die notwendigen Schritte für eine manuelle Konfiguration.

Abholung

Unter **Mails von diesem POP3-Server abholen** müssen Sie gegebenenfalls den POP3-Server angeben, von dem Sie die Mails abholen (z.B. *pop3.maildienstanbieter.de*).

Filter

Wenn **POP3-Mails** auf Grund einer Content-Prüfung oder auf Grund eines Virenbefalls zurückgewiesen werden, kann der Absender dieser Nachricht automatisch darüber informiert werden. Der **Ersatztext bei zurückgewiesenen Mails** lautet dabei: **Die Nachricht wurde vom Systemadministrator zurückgewiesen**. Sie können den Text für diese Benachrichtigungsfunktionen aber auch individuell gestalten. Dabei können Sie auch Platzhalter verwenden, die entsprechende Angaben zur zurückgewiesenen Mail in den Benachrichtigungstext übernehmen. Im frei definierbaren Text für den **Betreff** und den **Mailtext** stehen Ihnen folgende **Platzhalter** (definiert durch ein Prozentzeichen mit einem anschließenden Kleinbuchstaben) zur Verfügung:

- %v **Virus**
- %s **Absender**
- %r **Empfänger**
- %c **Cc**
- %d **Datum**
- %u **Betreff**
- %h **Header**
- %i **Absender-IP**

Virenprüfung

Bei der Virenprüfung haben Sie die Möglichkeit, Virenprüfungsoptionen für ein- und ausgehende Mails einzustellen:

Eingehend

Grundsätzlich sollten Sie natürlich die Funktion **Eingehende Mails auf Viren prüfen** aktiviert haben und auch darauf achten, welche Option Sie **im Falle einer Infektion** nutzen möchten.

- **Nur protokollieren**
- **Desinfizieren (wenn nicht möglich: nur protokollieren)**
- **Desinfizieren (wenn nicht möglich: umbenennen)**
- **Desinfizieren (wenn nicht möglich: löschen)**
- **Infizierte Anhänge umbenennen**
- **Infizierte Anhänge löschen**
- **Nachricht löschen**

Optionen, in denen nur ein **Protokollieren** eingehender Viren stattfindet, sollten Sie nur dann verwenden, wenn Sie Ihr System auf andere Weise permanent vor Virenbefall geschützt haben (z.B. mit dem Client/Server-basierten Virenschutz *G Data AntiVirus*). Bei **Virenfunden** haben Sie eine große Anzahl von **Benachrichtigungsoptionen**. So können Sie eine Virenwarnung in Betreff und Text der infizierten Mail einfügen, um den Empfänger einer solchen Mail zu informieren. Auch können Sie eine Meldung über den Virenfund an bestimmte Personen senden, also z.B. Systemverwalter oder zuständige Mitarbeiter davon in Kenntnis setzen, dass ein Virus an eine E-Mail-Adresse in ihrem Netzwerk verschickt wurde. Mehrere Empfängeradressen trennen Sie bitte mit einem Semikolon voneinander ab. Sie können den Text für die Benachrichtigungsfunktionen individuell gestalten. Dabei können Sie auch Platzhalter verwenden, die entsprechende Angaben zur zurückgewiesenen Mail in den Benachrichtigungstext übernehmen. Im frei definierbaren Text für den **Betreff** und den **Mailtext** stehen Ihnen folgende Platzhalter (definiert durch ein Prozentzeichen mit einem anschließenden Kleinbuchstaben) zur Verfügung:

- %v **Virus**
- %s **Absender**
- %r **Empfänger**
- %c **Cc**
- %d **Datum**
- %u **Betreff**

- %h **Header**
- %i **Absender-IP**

Ausgehend

Grundsätzlich sollten Sie natürlich die Funktion **Ausgehende Mails auf Viren prüfen** aktiviert haben und die Funktion **Infizierte Nachricht nicht versenden** standardmäßig eingeschaltet haben. Auf diese Weise verlässt kein Virus Ihr Netzwerk und richtet möglicherweise bei Geschäftspartnern Schaden. Bei Virenfunden haben Sie eine große Anzahl von **Benachrichtigungsoptionen**. So können Sie den **Absender der infizierten Mail benachrichtigen** und unter **Virenmeldung an folgende Personen senden** z.B. Systemverwalter oder zuständige Mitarbeiter davon in Kenntnis setzen, dass aus Ihrem Netzwerk ein Virus verschickt werden sollte. Mehrere Empfängeradressen trennen Sie bitte mit einem Semikolon voneinander ab. Sie können den Text für die Benachrichtigungsfunktionen individuell gestalten. Klicken Sie dazu einfach auf die **•••**-Schaltfläche rechts. Dabei können Sie auch **Platzhalter** verwenden, die entsprechende Angaben zur zurückgewiesenen Mail in den Benachrichtigungstext übernehmen. Im frei definierbaren Text für den **Betreff** und den **Mailtext** stehen Ihnen folgende Platzhalter (definiert durch ein Prozentzeichen mit einem anschließenden Kleinbuchstaben) zur Verfügung:

- %v **Virus**
- %s **Absender**
- %r **Empfänger**
- %c **Cc**
- %d **Datum**
- %u **Betreff**
- %h **Header**
- %i **Absender-IP**

Zusätzlich haben Sie unter **Bericht an ausgehende (nicht infizierte) Mails anhängen** die Möglichkeit, von *G Data MailSecurity* geprüfte Mails mit einem Bericht am Ende des Mailtextes zu versehen, in dem explizit darauf hingewiesen wird, dass diese Mail von *G Data MailSecurity* geprüft wurde. Selbstverständlich können Sie diesen Bericht aber auch individuell verändern oder ganz weglassen.

G Data AntiVirus Business

Wenn Sie den Client/Server basierten Virenschutz *G Data AntiVirus* (z.B. im Rahmen der *G Data AntiVirus Business*- oder *G Data AntiVirus Enterprise-Lösung*) installiert haben, können Sie über das Setzen des Häkchens bei **Virenfunde an G Data AntiVirus Business melden** dafür sorgen, dass die Client/Server-basierte Antivirensoftware *G Data AntiVirus* über Virenfunde des MailGateways benachrichtigt wird und Ihnen auf diese Weise einen umfassenden Überblick über die Virenbelastung bzw. -gefährdung Ihres Netzwerkes liefert.

Scanparameter

In diesem Bereich können Sie die Virenerkennungsleistung von *G Data MailSecurity* optimieren und an persönliche Erfordernisse anpassen. Generell gilt, dass durch eine Verringerung der Virenerkennungsleistung die Performance des Gesamtsystems steigt, während eine Erhöhung der Virenerkennungsleistung möglicherweise leichte Einbußen in der Performance mit sich bringen kann. Hier ist von Fall zu Fall abzuwägen. Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Engines benutzen:** *G Data MailSecurity* arbeitet mit zwei Antiviren-Engines, zwei grundsätzlich unabhängig voneinander operierenden Virenanalyseeinheiten. Unter **Engines benutzen** stellen Sie ein, wie diese miteinander kooperieren. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenprophylaxe. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich, d.h. wenn Sie nur eine Engine verwenden, kann der Analysevorgang schneller erfolgen.

- **Dateitypen:** Unter **Dateitypen** können Sie festlegen, welche Dateitypen von *G Data MailSecurity* auf Viren untersucht werden sollen. Wir empfehlen hier die automatische Typ-Erkennung über die automatisch nur die Dateien geprüft werden, die theoretisch auch einen Virus enthalten können. Wenn Sie selber die Dateitypen definieren möchten, für die eine Virenprüfung erfolgen soll, verwenden Sie die Funktion **benutzerdefiniert**. Durch Anklicken der **...**-Schaltfläche können Sie dann eine Dialogbox öffnen, in der Sie die gewünschten Dateitypen ins obere Eingabefeld eintragen und dann über die **Hinzufügen**-Schaltfläche in die Liste der benutzerdefinierten Dateitypen übernehmen. Sie können dabei auch mit **Platzhaltern** arbeiten, also Zeichen oder Zeichenketten durch die folgenden Symbole ersetzen:

Das Fragezeichen-Symbol (?) ist Stellvertreter für einzelne Zeichen.

Das Sternchen-Symbol (*) ist Stellvertreter für ganze Zeichenfolgen.

Um z.B. sämtliche Dateien mit der Dateiendung **exe** prüfen zu lassen, geben Sie also ***.exe** ein. Um z.B. Dateien unterschiedlicher Tabellenkalkulationsformate zu überprüfen (z.B. **xlr**, **xls**), geben Sie einfach ***.xl?** ein. Um z.B. Dateien unterschiedlichen Typs mit einem anfänglich gleichen Dateinamen zu prüfen, geben Sie beispielsweise **text*. *** ein.

- **Heuristik:** In der Heuristik-Analyse werden Viren nicht nur anhand der ständig aktualisierten Virendatenbanken, sondern auch anhand bestimmter virentypischer Merkmale ermittelt. Diese Methode ist einerseits ein weiteres Sicherheitsplus, andererseits kann sie in seltenen Fällen auch einen Fehlalarm erzeugen.
- **Archive prüfen:** Das Überprüfen **gepackter Dateien** in Archiven sollten generell aktiviert sein.
- **OutbreakShield:** Mit dem OutbreakShield können Schädlinge in Massenmails schon erkannt und bekämpft werden, bevor aktualisierte Signaturen dafür verfügbar sind. Das OutbreakShield erfragt dabei über das Internet besondere Häufungen von verdächtigen Mails und schließt dabei quasi in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Signaturen besteht. Wenn Sie **OutbreakShield** verwenden möchten, geben Sie über die Schaltfläche **Einstellungen** an, ob Sie einen Proxyserver verwenden und gegebenenfalls - um OutbreakShield einen jederzeitigen Zugang zum Internet zu ermöglichen - die **Zugangsdaten für die Internetverbindung**. Auf der Registerkarte **OutbreakShield** können Sie den Text der Mail definieren, den ein Mailempfänger enthält, wenn eine an ihn gerichtete Massenmail zurückgewiesen wurde.

Da das OutbreakShield auf Grund seiner eigenständigen Architektur infizierte Mailanhänge nicht desinfizieren, umbenennen oder in die Quarantäne verschieben kann, informiert der **Ersatztext** den Anwender darüber, dass ihm die verdächtige bzw. infizierte Mail nicht zugestellt wurde. Eine Meldung über vom OutbreakShield zurückgewiesene Mails entfällt, wenn Sie auf der Karteikarte **Virenprüfung** unter **Im Falle einer Infektion** den Punkt **Nachricht löschen** auswählen. In diesem Fall werden alle infizierten Mails, inklusive derer, die ausschließlich vom OutbreakShield erkannt werden, direkt gelöscht.

Warteschlange

In diesem Bereich können Sie festlegen, wie oft und in welchen Abständen der erneute Versand von Mails erfolgen soll, die vom MailGateway nicht an den entsprechenden Mail-Server weitergeleitet werden können.

Mails können sich dabei aus verschiedenen Gründen in der Warteschlange befinden. So kann z.B. der Mail-Server, an den Sie nach der Virenprüfung weitergeleitet werden sollen, überlastet oder ausgefallen sein.

Generell gelangen Mails erst nach der Virenüberprüfung durch *G Data MailSecurity* in die Warteschlange.

Nicht zustellbare Nachrichten

Geben Sie unter **Wiederholungsintervall** an, in welchen Abständen *G Data MailSecurity* einen neuen Versendeversuch unternehmen soll. So bedeutet z.B. die Angabe **1, 1, 1, 4**, dass *G Data MailSecurity* die ersten drei Stunden stündlich versucht, die Mail zu verschicken und von da an regelmäßig im Abstand von 4 Stunden. Unter **Fehlerwartezeit** legen Sie fest, wann die Versendung der Mail endgültig abgebrochen und die Mail gelöscht wird. Sie können **Absender von Nachrichten in der Warteschlangen alle x Stunden benachrichtigen**, wobei **x** ein ganzzahliger Stundenwert sein muss. Wenn Sie die Absender einer nicht zustellbaren Nachricht nicht regelmäßig informieren möchten, geben Sie hier einfach eine **0** ein.

Auch wenn Sie die regelmäßige Benachrichtigung von Absendern nicht weitergeleiteter Mails abschalten, wird der Absender natürlich dennoch informiert, wenn seine Mail endgültig nicht zugestellt und vom Server gelöscht wurde.

Über die Schaltfläche **Auf Standardwerte zurücksetzen** können Sie die Standardeinstellungen im Bereich Warteschlange wiederherstellen. Diese Einstellungen haben sich in der Praxis bewährt.

Größenbegrenzung

Die Größe der Warteschlange kann auf Wunsch begrenzt werden. Dies dient dem Schutz vor **Denial of Service-Attacken**. Sollte die Größenbeschränkung überschritten werden, werden keine weiteren Mails mehr in die Warteschlange aufgenommen.

Erweitert

Im **Erweitert**-Bereich können Sie globale Einstellungen von *G Data MailSecurity* verändern.

Rechnername

Hier können Sie ggf. den Rechnernamen (**FQDN = Full Qualified Domain Name**) des Mailservers ändern.

Begrenzung

Um die Anzahl der SMTP-Verbindungen zu begrenzen, die *G Data MailSecurity* gleichzeitig verarbeitet, setzen Sie bitte das Häkchen vor **Anzahl von SMTP Client-Verbindungen begrenzen**. *G Data MailSecurity* lässt dann nur die maximale Zahl von Verbindungen zu, die Sie vorgeben. Auf diese Weise können Sie die Mailfilterung an die Leistung der Hardware anpassen, die Sie für das MailGateway verwenden.

Systemnachrichten

Die Absenderadresse für Systemnachrichten ist die Mail-Adresse, die z.B. dazu verwendet wird, Absender und Empfänger virenfizierter Mails zu informieren oder darüber zu informieren, dass sich ihre Mails in der Warteschlange befinden. *G Data MailSecurity* Systemwarnungen sind unabhängig von den allgemeinen Mitteilungen bei Virenfunden. Bei einer **Systemwarnung** handelt es sich in der Regel um eher globale Informationen, die nicht mit einer einzelnen möglicherweise infizierten Mail in Zusammenhang stehen. So würde *G Data MailSecurity* z.B. eine Systemwarnung verschicken, wenn die Virenkontrolle aus irgendwelchen Gründen nicht mehr gewährleistet ist. Die Empfängeradresse(n) für Systemwarnungen können durchaus identisch mit den Adressen sein, die Sie unter **Eingehend/Ausgehend (SMTP, POP3)** verwenden.

Einstellungen

Über die Schaltflächen **Import** und **Export** können Sie die Einstellungen der Programm-Optionen auch als **XML-Datei** speichern und so ggf. erneut einspielen, wenn der Bedarf gegeben ist.

Kennwort ändern

Hier können Sie das **Administrator-Passwort** ändern, das Sie beim ersten Start von *G Data MailSecurity* vergeben haben. Geben Sie dazu einfach das momentan aktuelle Passwort unter **Altes Kennwort** ein und dann unter **Neues Kennwort** und **Neues Kennwort bestätigen** das neue Kennwort. Mit Anklicken der **OK**-Schaltfläche wird die Kennwortänderung durchgeführt.

Logging

Im **Logging**-Bereich können Sie den Mailverkehr auf Ihrem Server statistisch auswerten. Die Ergebnisse dieser Statistikfunktion können Sie im Statistik-Bereich der Programmoberfläche aufrufen, den Sie durch Anklicken der Schaltfläche **Statistik** im Programmbereich **Status** finden. Alternativ können Sie die ermittelten Daten auch in einer externen Log-Datei (maillog.txt) abspeichern. Über die Funktionen **Nur Junk-Mails** und **Anzahl von E-Mails begrenzen** können Sie die Größe dieser Log-Datei gegebenenfalls begrenzen.

Update

Im Update-Bereich können Sie umfangreiche Einstellungen vornehmen, um *G Data MailSecurity* optimal auf die Gegebenheiten anzupassen, die in Ihrem Netzwerk existieren. Hier können Sie die Virensignaturen und Programmdateien von *G Data MailSecurity* manuell oder automatisiert auf den neuesten Stand bringen.

Einstellungen

Hier können Sie grundlegende Einstellungen für das Internet Update vorgeben. Wenn Sie (z.B. im Rahmen der *G Data AntiVirus Business-Lösung*) parallel zu *G Data MailSecurity* das Client/Server-basierte *G Data AntiVirus* verwenden, können Sie sich über **Virensignaturen vom G Data Security Client verwenden** den doppelten Download der Virensignaturen sparen und diese direkt von **G Data AntiVirus** erhalten, das diese schon auf Ihrem Server gespeichert hat. Über **Internet Update der Virensignaturen selbst durchführen** führt *G Data MailSecurity* diesen Vorgang selbstständig durch. Über die Schaltfläche **Einstellungen und Zeitplanung** gelangen Sie in einen Bereich, in dem Sie sämtliche notwendigen Einstellungen für manuelle und automatische Internet Updates eingeben können.

Zugangsdaten

Geben Sie unter **Zugangsdaten** den Benutzernamen und das Passwort ein, das Sie bei der Anmeldung von *G Data MailSecurity* erhalten haben. Klicken Sie auf die Schaltfläche **Am Server anmelden**, wenn Sie sich noch nicht am *G Data*-Server angemeldet haben. Mit Hilfe dieser Daten werden Sie vom *G Data*-Server erkannt und das Update der Virensignaturen kann vollautomatisch erfolgen.

Wenn Sie noch keine **Anmeldung am Server** durchgeführt haben, können Sie diese jetzt nachholen. Geben Sie einfach die Anmelde Nummer ein (- Sie finden diese auf der Rückseite des Benutzerhandbuches -), Ihre Kundendaten und klicken Sie auf **Senden**. Sofort werden Ihnen die Zugangsdaten (Benutzername und Passwort) angezeigt. Sie sollten sich diese Daten aufschreiben und diese sicher verwahren. Für die Anmeldung am Server ist natürlich (- wie auch für das Internet Update der Virensignaturen -) eine Internetverbindung notwendig.

Zeitplanung Viren-Update

Über die Karteikarte **Zeitplanung Viren-Update** können Sie festlegen, wann und in welchem Rhythmus das automatische Update erfolgen soll. Unter **Ausführen** geben Sie dazu eine Vorgabe vor, die Sie dann mit den Eingaben unter **Zeitpunkt** spezifizieren.

Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** z.B. bestimmen, dass Ihr Rechner nur an Werktagen das Update durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird. Um unter **Zeitpunkt** Daten- und Zeiteinträge zu ändern, markieren Sie einfach das Element, das Sie ändern möchten (z.B. Tag, Stunde, Monat, Jahr) mit der Maus und nutzen dann die Pfeiltasten oder die kleinen Pfeilsymbole rechts vom Eingabefeld, um sich im jeweiligen Element chronologisch zu bewegen.

Internet-Einstellungen

Falls Sie einen Rechner hinter einer **Firewall** verwenden oder andere besondere Einstellungen bezüglich Ihres Internetzugangs haben, verwenden Sie bitte einen **Proxyserver**. Sie sollten diese Einstellung nur ändern, wenn das Internet Update nicht funktioniert. Wenden Sie sich wegen der Proxy-Adresse gegebenenfalls an Ihren Internetzugangsanbieter.

Die Zugangsdaten für die Internetverbindung (Benutzernamen und Passwort) sind gerade beim automatischen Internet Update per Zeitplan sehr wichtig. Ohne diese Angaben kann keine automatische Verbindung mit dem Internet erfolgen. Achten Sie bitte auch darauf, dass Sie in Ihren allgemeinen Interneteinstellungen (z.B. für Ihr Mailprogramm oder Ihren Internetbrowser) die **automatische Einwahl** ermöglichen. Ohne die automatische Einwahl startet *G Data MailSecurity* zwar den Internet Update-Vorgang, muss dann aber darauf warten, dass Sie den Aufbau der Internetverbindung mit **OK** bestätigen.

Über die Auswahl unter **Updateserver-Region** können Sie einen Updateserver in Ihrer Region auswählen, um ggf. die Datenübermittlung zu optimieren.

Benutzerkonto

Geben Sie bitte unter **Benutzerkonto** ein Benutzerkonto auf dem MailGateway-Rechner an, für das ein Zugang zum Internet besteht.

Achtung: Bitte verwechseln Sie nicht die Angaben, die Sie in den Karteikarten **Zugangsdaten** und **Benutzerkonto** tätigen.

Virensignaturen

Über die Schaltflächen **Viren-Update** und **Status aktualisieren** können Sie auch unabhängig von den Vorgaben, die Sie unter Zeitplanung vorgenommen haben, ein aktuelles Virensignaturupdate starten.

Programmdateien

Über die Schaltfläche **Programm-Update** können Sie auch die Programmdateien von *G Data MailSecurity* aktualisieren, sobald sich hier Änderungen und Verbesserungen ergeben.

Spam-Filter

Über den Spam-Filter haben Sie umfangreiche Einstellungsmöglichkeiten, um Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren. Das Programm prüft viele Merkmale der Mails, die typisch für Spam sind. Anhand der zutreffenden Merkmale wird ein Wert errechnet, der die Wahrscheinlichkeit für Spam widerspiegelt. Dazu stehen Ihnen mehrere Karteikarten zur Verfügung, in denen Ihnen alle relevanten Einstellungsmöglichkeiten thematisch gegliedert zur Verfügung stehen.

Filter

Geben Sie unter **Name** und **Bemerkung** an, wie Sie den Filter nennen möchten und welche zusätzlichen Informationen hierzu vielleicht nötig sind. Unter **Reaktion** können Sie bestimmen, wie der Spam-Filter mit Mails umgehen soll, die möglicherweise Spam enthalten. Dabei können Sie drei Abstufungen vornehmen, die davon beeinflusst werden, wie hoch *G Data MailSecurity* die Wahrscheinlichkeit dafür ansetzt, dass es sich bei der betreffenden E-Mail um Spam handelt.

Unter **Spamverdacht** wird der Umgang mit den Mails geregelt, in denen *G Data MailSecurity* einzelne Spam-Elemente findet. Dabei muss es sich nicht generell um **Spam** handeln, sondern in seltenen Fällen möglicherweise auch um Newsletter-Mails oder Sammelmailings, die vom Empfänger durchaus erwünscht sind. Hier empfiehlt es sich, den Empfänger auf den Spam-Verdacht hinzuweisen. Unter **Hohe Spamwahrscheinlichkeit** werden die Mails zusammengefasst, die viele Merkmale für Spam in sich vereinen und nur in sehr seltenen Fällen vom Empfänger wirklich erwünscht sind. Unter **Sehr hohe Spamwahrscheinlichkeit** finden sich die Mails, die alle Kriterien einer Spam-Mail erfüllen. Hier handelt es sich so gut wie nie um gewünschte E-Mails und das Zurückweisen von derart gestalteten Mails ist in den meisten Fällen empfehlenswert.

Mit einer **Weiterleitung** solcher Mails an **G Data** verbessern Sie die Spamerkennung! Sie können diese Option aber natürlich auch abschalten.

Jede dieser drei abgestuften Reaktionen können Sie individuell gestalten.

So haben Sie über **Mail zurückweisen** die Möglichkeit, die Mail gar nicht erst auf Ihren Mail-Server gelangen zu lassen. Der Empfänger erhält diese Mail dann erst gar nicht. Über **Spamwarnung in Betreff und Text der infizierten Mail einfügen** können Sie einen Empfänger einer als Spam identifizierten Mail davon in Kenntnis setzen, dass es sich um Spam handelt. Über die Option **Absender der Nachricht benachrichtigen** können Sie eine automatische Antwortmail an den Absender der als Spam erkannten Mail verschicken, in der Sie diesen darauf hinweisen können, dass seine Mail als Spam erkannt wurde. Da gerade bei Spam viele Mailadressen aber nur einmal verwendet werden, sollten Sie sich überlegen, ob Sie diese Funktion aktivieren. Über die Option **An folgende Personen weiterleiten** können Sie als Spam verdächtige Mails auch automatisch weiterleiten, z.B. an den Systemadministrator.

Whitelist

Über die Whitelist können Sie bestimmte Absender-Adressen oder Domains explizit vom Spamverdacht ausnehmen. Geben Sie dazu einfach in das Feld **Adressen/Domains** die gewünschte E-Mail-Adresse (z.B. *newsletter@gdata.de*) oder Domain (z.B. *gdata.de*) ein, die Sie vom Spamverdacht ausnehmen möchten und *G Data MailSecurity* behandelt Mails von diesem Absender bzw. dieser Absenderdomain nicht als Spam. Über die **Import**-Schaltfläche können Sie auch vorgefertigte Listen von E-Mail-Adressen oder Domains in die Whitelist einfügen. Die Adressen und Domains müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows Notepad erstellt werden kann. Über die **Export**-Schaltfläche können Sie eine solche Whitelist auch als Textdatei exportieren.

Blacklist

Über die Blacklist können Sie bestimmte Absender-Adressen oder Domains explizit unter Spamverdacht setzen. Geben Sie dazu einfach in das Feld **Adressen/Domains** die gewünschte E-Mail-Adresse (z.B. *newsletter@megaspam.de.vu*) oder Domain (z.B. *megaspam.de.vu*) ein, die Sie unter Spamverdacht setzen möchten und *G Data MailSecurity* behandelt Mails von diesem Absender bzw. dieser Absenderdomain generell als **Mails mit sehr hoher Spamwahrscheinlichkeit**. Über die **Import**-Schaltfläche können Sie auch vorgefertigte Listen von E-Mail-Adressen oder Domains in die Blacklist einfügen. Die Adressen und Domains müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows Notepad erstellt werden kann. Über die **Export**-Schaltfläche können Sie eine solche Blacklist auch als Textdatei exportieren.

Realtime Blacklists

Im Internet finden sich schwarze Listen, die IP-Adressen von Servern enthalten, über die bekanntermaßen Spam verschickt wird. *G Data MailSecurity* ermittelt durch DNS-Anfragen an die **RBLs (Realtime Blacklists)**, ob der sendende Server gelistet ist. Falls ja, erhöht sich die Spamwahrscheinlichkeit. Generell sollten Sie hier die Standardeinstellung verwenden, können allerdings auch unter **Blacklist 1, 2 und 3** eigene Adressen für **Blacklists** aus dem Internet vergeben.

Schlüsselwörter (Betreff)

Über die Liste der Schlüsselwörter können Sie Mails auch anhand der in der **Betreffzeile** verwendeten Wörter unter Spamverdacht stellen. Wenn mindestens einer der Begriffe in der Betreffzeile vorkommt, erhöht sich die Spamwahrscheinlichkeit. Diese Liste können Sie über die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** beliebig verändern. Über die **Import**-Schaltfläche können Sie auch vorgefertigte Listen von Schlüsselwörtern in Ihre Liste einfügen. Die Einträge müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows Notepad erstellt werden kann. Über die **Export**-Schaltfläche können Sie eine solche Liste von Schlüsselwörtern auch als Textdatei exportieren. Über das Häkchen vor **Nur vollständige Wörter suchen** können Sie festlegen, dass *G Data MailSecurity* die Betreffzeile einer Mail nur nach ganzen Wörtern durchsucht, so würde z.B. ein Begriff wie *cash* unter Spamverdacht fallen, während z.B. die gemeinen *Cashew-Kerne* weiterhin unbeanstandet bleiben.

Schlüsselwörter (Mailtext)

Über die Liste der Schlüsselwörter können Sie Mails auch anhand der im **Mailtext** verwendeten Wörter unter Spamverdacht stellen. Wenn mindestens einer der Begriffe im Mailtext vorkommt, erhöht sich die Spamwahrscheinlichkeit. Diese Liste können Sie über die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** beliebig verändern.

Über die **Import**-Schaltfläche können Sie auch vorgefertigte Listen von Schlüsselwörtern in Ihre Liste einfügen. Die Einträge müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows Notepad erstellt werden kann.

Über die **Export**-Schaltfläche können Sie eine solche Liste von Schlüsselwörtern auch als Textdatei exportieren. Über das Häkchen vor **Nur vollständige Wörter suchen** können Sie festlegen, dass *G Data MailSecurity* die Betreffzeile einer Mail nur nach ganzen Wörtern durchsucht, so würde z.B. ein Begriff wie *cash* unter Spamverdacht fallen, während z.B. die gemeinen *Cashew-Kerne* weiterhin unbeanstandet bleiben.

Inhaltsfilter

Beim Inhaltsfilter handelt es sich um einen selbstlernenden Filter auf Basis der Bayes-Methode, der auf Grund der im Mailtext verwendeten Worte eine Spamwahrscheinlichkeit berechnet. Dabei arbeitet dieser Filter nicht allein auf Basis feststehender Wortlisten, sondern lernt bei jeder neu empfangenen Mail weiter dazu. Über die Schaltfläche **Tabelleninhalte abfragen** können Sie sich die Wortlisten anzeigen lassen, die der Inhaltsfilter zur Einordnung einer Mail als Spam verwendet. Über die Schaltfläche **Tabellen zurücksetzen** löschen Sie alle gelernten Tabelleninhalte und der selbstlernende Inhaltsfilter startet den Lernvorgang erneut von Beginn an.

Profi-Einstellungen

In diesem Bereich können Sie die Spamerkennung von *G Data MailSecurity* sehr detailliert verändern und an die Gegebenheiten Ihres Mail-Servers anpassen. Generell empfiehlt es sich hier jedoch, die Standardeinstellungen zu verwenden. In den Profi-Einstellungen sollten Sie nur dann Veränderungen vornehmen, wenn Sie sich in der Thematik auskennen und genau wissen, was Sie tun.

10 FAQ Installation

10.1 Ich habe die G Data Software ohne Registrierung installiert. Wie kann ich die Software registrieren?

Um die Software nachträglich zu registrieren, öffnen Sie unter Start > Alle Programme > G Data > G Data ManagementServer das **Internet-Update**. Dort steht die Option **Online-Registrierung** zur Verfügung. Nach einem Klick auf diese Schaltfläche öffnet sich das Registrierungsformular. Geben Sie dort die Registriernummer ein, die dem Produkt beiliegt. Sie finden diese je nach Art des Produktes auf der Lizenzurkunde (MediaPack) oder in der Auftragsbestätigung. Kontaktieren Sie im Zweifelsfall Ihren Händler bzw. den betreuenden Distributor.

Durch die Eingabe der Registrierungsnummer wird Ihr Produkt aktiviert. Die erstellten Zugangsdaten werden Ihnen nach erfolgter Registrierung angezeigt. **Notieren Sie sich unbedingt diese Zugangsdaten!** Nach erfolgter Registrierung ist eine erneute Eingabe des Lizenzschlüssels nicht mehr möglich. Sollten Sie bei der Eingabe der Registriernummer Probleme haben, überprüfen Sie die Registriernummer auf die korrekte Eingabe. Je nach verwendeten Schriftsatz wird ein großes "I" (wie Ida) oft als die Ziffer "1", bzw. dem Buchstaben "l" (wie Ludwig) fehlinterpretiert. Das Gleiche gilt für: "B" und "8", "G" und 6, "Z" und "2".

Sollten Sie eine G Data ClientSecurity, eine G Data EndpointProtection oder als Zusatzmodul einen G Data PatchManager erworben und bei der Installation nicht aktiviert haben, werden die Karteireiter **Firewall**, **PatchManager** und **PolicyManager** erst nach erfolgreicher Aktivierung freigeschaltet. Bis dahin stehen nur die Funktionen von G Data AntiVirus Business zur Verfügung.

10.2 Ich möchte die Installation der Clients zentral vom Server aus über den G Data Administrator durchführen

Am komfortabelsten ist die **Installation über den G Data Administrator**. Lesen Sie hierzu bitte das Kapitel: **G Data Client installieren**.

- 1** Damit die Clients den Server erreichen können, muss auf dem Server der **Port 7161 (TCP)** erreichbar sein.
- 2** Um die Kommunikation vom Server zum Client zu gewährleisten, muss auf dem Client **Port 7167 (TCP)** freigegeben sein.

Um die Kommunikation zwischen Clients zu gewährleisten (P2P Update Verteilung), muss auf dem Client Port 7169
- 3** Sofern eine Firewall verwendet wird, muss für die Datei **gdmms.exe** eine **Ausnahme** definiert sein.
- 4** In einer Windows-Arbeitsgruppe muss unter Windows XP die **einfache Dateifreigabe**, unter Windows Vista bzw. Windows 7 die Option **Freigabeassistent verwenden** deaktiviert werden. Zusätzlich sollte die Benutzerkontensteuerung (UAC) deaktiviert sein.
- 5** Ein Zugriff auf die Freigaben C\$ und Admin\$ des Clients ist erforderlich.
- 6** Es muss ein **Passwort** vergeben sein. Ein leeres Passwort ist nicht zulässig.
- 7** In den **Diensten** muss der **Remoteregistrierungsdienst** aktiv sein.

Die **Remote-Installation** kann in zwei Varianten durchgeführt werden. Wenn der Client die Voraussetzungen dafür erfüllt, werden die Dateien direkt kopiert und die Einträge in der Registry vorgenommen. Kann der Server nur auf die Festplatte aber nicht auf die Registry zugreifen oder sind andere Systemvoraussetzungen nicht erfüllt, wird das komplette Setup-Programm auf den Client kopiert und beim nächsten Hochfahren des Computers automatisch gestartet. Zur Installation begeben Sie sich einfach in der Menüleiste des G Data Administrators und rufen dort die Funktion **Clients > G Data Client installieren** auf. Es erscheint ein Eingabefenster, in dem Sie Benutzername, Passwort und Domäne des G Data ManagementServers angeben. Nach Eingabe dieser Daten erscheint ein Fenster mit allen verfügbaren Netzwerkrechnern. Aktivierte Clients sind dabei mit einem Symbol gekennzeichnet. Deaktivierte Clients werden durch ein schattiertes Symbol dargestellt. Wählen Sie zur Installation einen Netzwerkrechner aus und klicken dann auf die Schaltfläche **Installieren**. Auf diese Weise wird der G Data Security Client auf diesem Rechner installiert. Sollte Ihr System nicht die Voraussetzungen für eine Remote-Installation der G Data Client-Software erfüllen, haben Sie natürlich auch die Möglichkeit, die Clients manuell oder halbautomatisch mit der G Data Client-Software zu versehen.

10.3 Ich möchte den G Data Administrator auf einem Client-Rechner installieren

Sie können den **G Data Administrator** natürlich auch von jedem anderen Computer im Netzwerk starten.

Die Installation des G Data Administrators auf den angeschlossenen Clientrechnern ist für die reibungslose Funktion nicht erforderlich.

Eine Installation des G Data Administrators auf einem Client-Rechner empfiehlt sich, wenn vor Ort ein Zugriff auf die Einstellungen des G Data ManagementServers benötigt wird.

Wir empfehlen dazu, das Verzeichnis **Admin** freizugeben und dann die Datei **Admin.exe** von dem anderen Computer aufzurufen. Natürlich können Sie die Datei auch auf andere Computer kopieren und von dort starten. Die Freigabe hat den Vorteil, dass Sie immer die neueste Version starten, da die Datei durch ein Internet-Update aktualisiert werden kann. Wahlweise können Sie deshalb auch die G Data-DVD in das DVD-Laufwerk des Client-Rechners einlegen, die Schaltfläche **Installieren** drücken und anschließend die Komponente G Data Administrator durch einen Klick auf die entsprechende Schaltfläche auswählen. Im folgenden Begrüßungsbildschirm werden Sie darüber informiert, dass Sie im Begriff sind den G Data Administrator auf Ihrem System zu installieren. Schließen Sie spätestens jetzt alle offenen Anwendungen in Ihrem Windows-System, da diese sonst zu Problemen bei der Installation führen könnten. Klicken Sie auf **Weiter**, um mit der Installation fortzufahren. Der nächste Bildschirm ermöglicht Ihnen die Auswahl des Ortes, an dem die Daten des G Data Administrators abgespeichert werden sollen. Standardmäßig wird der G Data Administrator unter **C:\Programme\G DATA\G DATA AntiVirus ManagementServer\Admin** abgelegt. Sollten Sie einen anderen Speicherort auswählen wollen, haben Sie die Möglichkeit über die Schaltfläche **Durchsuchen** eine Verzeichnisansicht zu öffnen, in der Sie ein anderes Verzeichnis auswählen oder auch neu anlegen können. Mit **Weiter** gelangen Sie zum nächsten Installationsschritt. Nun haben Sie die Möglichkeit, eine Programmgruppe auszuwählen. Wenn Sie auf **Weiter** klicken, finden Sie das Programm standardmäßig in der Programmgruppe **G Data\G Data Administrator** in der Programmauswahl des Windows-Startmenüs. Die Installation wird mit einem Abschlussbildschirm beendet. Klicken Sie auf **Beenden**. Der G Data Administrator steht Ihnen nun zur Verfügung. Sie können das Administrator-Tool zur Steuerung des G Data ManagementServers mit einem Klick auf den Eintrag **G Data Administrator** in der Programmgruppe **Start > Programme > G Data > G Data Administrator** des Startmenüs aufrufen.

10.4 Ich möchte die Clients mit Hilfe der G Data-CD-ROM mit der Client-Software ausstatten

Sie können die Client-Software auch direkt auf den einzelnen Clients von der mitgelieferten DVD installieren. Legen Sie dazu die DVD in das DVD-Laufwerk des Client-Rechners, wählen dann die Komponente **G Data Security Client** mit einem Klick auf die nebenstehende Schaltfläche aus. Bei der Installation werden Sie dann nach dem Namen des Computers gefragt, auf dem der G Data ManagementServer installiert ist. Geben Sie den entsprechenden Namen (z.B. **avk_server**) ein. Mit Betätigung der **Weiter**-Schaltfläche schließen Sie die Installation ab. Sollte das Setup-Programm auf dem Abschlussbildschirm einen Neustart des Computers vorschlagen, führen Sie diesen durch, da der Client in diesem Fall erst nach einem Neustart funktionsfähig ist.

10.5 Nach der Installation des Clients laufen einige Anwendungen erheblich langsamer als vorher

Der Wächter überwacht im Hintergrund alle Dateizugriffe und prüft im Zugriff befindliche Dateien auf Viren. Dieses führt normalerweise zu einer kaum spürbaren *Verzögerung*. Falls eine Anwendung sehr viele Dateien oder einige Dateien sehr oft öffnet, kann eine erhebliche Verzögerung auftreten. Um dies zu umgehen, deaktivieren Sie den Wächter zunächst temporär, um herauszufinden, ob die Verzögerungen durch ihn hervorgerufen werden. Wenn der betroffene Rechner auf Dateien eines Servers zugreift, muss auch der Wächter auf dem Server temporär deaktiviert werden. Falls der Wächter die Ursache ist, kann das Problem i.d.R. durch die Definition einer *Ausnahme* (= Dateien, die nicht geprüft werden sollen) behoben werden. Dazu müssen zunächst die Dateien ermittelt werden, auf die häufig zugegriffen wird. Mit einem Programm wie z.B. *MonActivity* können diese Daten ermittelt werden. Wenden Sie sich hierzu ggf. an unser **ServiceCenter**.

Selbstverständlich können Sie auch die Performance dadurch steigern, indem Sie nicht beide Engines zur Virenüberprüfung verwenden, sondern nur eine Engine. Dies bietet sich in erster Linie auf älteren Systemen an.

11 FAQ Allgemeines

Geben Sie hier den Text ein.

11.1 MailSecurity, Exchange-Server 2000 und AVM

Ken!
Ich verwende AVM Ken! und möchte G Data MailSecurity auf dem gleichen Rechner wie den Ken!-Server installieren:

Detaillierte Anleitungen hierzu erhalten Sie von unserem **Support-Team**.

Ich verwende einen Exchange-Server 2000 und möchte G Data MailSecurity auf dem gleichen Rechner wie den Exchange-Server installieren. Wie kann ich im Exchange-Server die Ports für eingehende und ausgehende Mails umstellen?

Detaillierte Anleitungen hierzu erhalten Sie von unserem **Support-Team**.

11.2 Wie kann ich überprüfen, ob die Clients eine Verbindung zum G Data ManagementServer haben?

Die Spalte **Letzter Zugriff** im Aufgabenbereich **Clients** enthält den Zeitpunkt, an dem sich der Client zum letzten Mal beim G Data ManagementServer gemeldet hat. In der Standardeinstellung melden sich die Clients alle fünf Minuten beim G Data ManagementServer (wenn gerade keine Scanaufträge ausgeführt werden). Folgende Ursachen können für eine fehlgeschlagene Verbindung verantwortlich sein:

- Der Client ist ausgeschaltet oder vom Netzwerk getrennt.
- Es kann keine TCP/IP-Verbindung zwischen dem Client und dem G Data ManagementServer aufgebaut werden. Prüfen Sie die Netzwerkeinstellungen bzw. Portfreigaben.
- Der Client kann die IP-Adresse des Servers nicht ermitteln, d.h. die DNS Namensauflösung funktioniert nicht. Die Verbindung kann mit dem Befehl **telnet** über die Eingabeaufforderung überprüft werden. Am **Server** muss **TCP Port 7161** erreichbar sein, am **Client** muss **TCP Port 7167** bzw. **TCP Port 7169** erreichbar sein. Prüfen Sie die Verbindung mit dem Befehl **telnet <SERVERNAME> <PORTNUMMER>**

Beachten Sie, dass unter **Windows Vista**, **Windows 7** sowie **Server 2008 (R2)** der telnet-Befehl standardmäßig nicht verfügbar ist. Aktivieren Sie daher die entsprechende Windows-Funktion bzw. fügen Sie sie als neues Feature zum Server hinzu. Ist die Verbindung vom Client zum Server intakt, erscheint in der Eingabeaufforderung eine Sammlung kryptischer Zeichen. Wenn die Verbindung vom Server zum Client intakt ist, erscheint ein leeres Eingabefenster.

11.3 Mein Postfach wurde in die Quarantäne geschoben

Dies passiert, wenn sich in dem Postfach eine infizierte Mail befindet. **Zurückbewegen der Datei:** Schließen Sie das Mailprogramm auf dem betroffenen Client und löschen Sie eine evt. neu angelegte Archivdatei. Öffnen Sie anschließend im G Data Administrator den zugehörigen Bericht und klicken Sie auf **Datei zurückbewegen**. Kontaktieren Sie bitte unseren Support, wenn das Zurückbewegen fehlschlägt.

11.4 Der MMS soll nicht über seinen Namen, sondern über die IP-Adresse angesprochen werden

Installation des G Data ManagementServers: Bei der Installation wird nach dem Servernamen gefragt. Der Name muss durch die **IP-Adresse** ersetzt werden. Sie können den Servernamen auch nachträglich durch die IP-Adresse ersetzen, wenn der G Data ManagementServer bereits installiert ist. Passen Sie dazu - je nach Ihrem System - einen dieser Registry-Einträge an:

HKEY_LOCAL_MACHINE\SOFTWARE\G DATA\AVK ManagementServer\ComputerName

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\G DATA\AVK ManagementServer\ComputerName

Aktivierung der Clients im G Data Administrator: Damit die Verbindung vom Server zu den Clients auch über die IP-Adresse hergestellt werden kann, müssen die Clients im G Data Administrator mit Ihrer IP-Adresse aktiviert werden. Das geht entweder von Hand (**Clients/Client aktivieren (Dialog)**) oder durch **Active Directory Synchronization**.

G Data Client-Setup von der DVD: Wenn die Clients direkt von der DVD installiert werden, fragt das Installationsprogramm sowohl nach dem Servernamen als auch nach dem Computernamen. Geben Sie hier jeweils die IP-Adresse ein.

11.5 Speicherorte und Pfade

Virensignaturen G Data Security Client:

- XP / Server 2003 / Server 2003 R2: C:\Programme\Gemeinsame Dateien\G DATA\AVKScanP\AVAST5 bzw. BD
- Vista / Win7 / Win8 / Server 2008 / Server 2008 R2 / Server 2012: C:\Programme (x86)\Common Files\G DATA\AVKScanP\AVAST5 bzw. BD

Virensignaturen G Data ManagementServer

- XP / Server 2003 / Server 2003 R2: C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\G DATA\AntiVirus ManagementServer\Updates
- Vista / Win7 / Win8 / Server 2008 / Server 2008 R2 / Server 2012: C:\ProgramData\G DATA\AntiVirus ManagementServer\Updates

G Data Security Client-Quarantäne

- XP / Server 2003 / Server 2003 R2: C:\Programme\Gemeinsame Dateien\G DATA\AVKScanP\QBase
- Vista / Win7 / Win8 / Server 2008 / Server 2008 R2 / Server 2012: C:\Programme (x86)\Common Files\G DATA\AVKScanP\QBase

G Data ManagementServer-Quarantäne

- XP / Server 2003 / Server 2003 R2: C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\G DATA\AntiVirus ManagementServer\Quarantine
- Vista / Win7 / Win8 / Server 2008 / Server 2008 R2 / Server 2012: C:\ProgramData\G DATA\AntiVirus ManagementServer\Quarantine

MMS-Datenbanken (integriert; nur bis einschl. Version 10.7)

- XP / Server 2003 / Server 2003 R2: C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\G DATA\AntiVirus ManagementServer\Database
- Vista / Win7 / Win8 / Server 2008 / Server 2008 R2 / Server 2012: C:\ProgramData\G DATA\AntiVirus ManagementServer\Database

MMS-Datenbanken (SQL)

XP / Server 2003 / Server 2003 R2 / Vista / Win7 / Win8 / Server 2008 / Server 2008 R2 / Server 2012:

- C:\Programme\Microsoft SQL Server\MSSQL.1\MSSQL\Data\GDATA_AntiVirus_ManagementServer.mdf
- C:\Programme\Microsoft SQL Server\MSSQL.1\MSSQL\Data\GDATA_AntiVirus_ManagementServer_log.ldf

12 FAQ Linux-Nutzung

Geben Sie hier den Text ein.

12.1 Linux-Fileserver Clients: Es wird keine Verbindung zum G Data ManagementServer aufgebaut / Signaturen werden nicht aktualisiert

- 1** Prüfen Sie ob die beiden Prozesse des G Data Linux-Clients laufen: Geben Sie im Terminal

```
linux:~# ps ax|grep av
```

ein. Sie sollte die Ausgaben

```
... Ssl 0:07 /usr/sbin/avkserver --daemon  
... Ssl 0:05 /usr/sbin/avclient --daemon
```

erhalten. Sie können die Prozesse unabhängig von der eingesetzten Distribution mit

```
linux:~# /etc/init.d/avkserver start  
linux:~# /etc/init.d/avclient start
```

starten und mit

```
linux:~# /etc/init.d/avkserver stop  
linux:~# /etc/init.d/avclient stop
```

anhalten. Hierzu müssen Sie als Administrator (= "root") auf dem Linux-Rechner eingeloggt sein.
- 2** Sehen Sie sich die Log-Dateien an: Unter **/var/log/** befindet sich die Log-Datei **gdata_install.log**. In dieser Datei wird der Verlauf der Remote-Installation protokolliert. Im Verzeichnis **/var/log/gdata** befindet sich die Log-Datei **avkclient.log**. In dieser Log-Datei werden die Scan-Ergebnisse des Scanners **avkserver** und die Ausgaben des Prozesses **avclient** protokolliert, der die Verbindung zum G Data ManagementServer herstellt. Schauen Sie sich die Dateien an und suchen Sie nach Fehlermeldungen. Wenn Sie mehr Meldungen sehen möchten, können Sie in den Konfigurationsdateien **/etc/gdata/gdav.ini** und **etc/gdata/avclient.cfg** die Einträge für **LogLevel** auf den Wert **7** setzen.

Vorsicht: Hohe LogLevel erzeugen viele Meldungen und lassen die Log-Dateien schnell anwachsen. Setzen Sie die LogLevel im Normalbetrieb immer auf niedrige Werte!
- 3** Testen Sie den Scanner: Mit dem Kommandozeilen-Tool **avkclient** können sie die Funktion des Scanservers **avkserver** testen. Folgende Kommandos lassen sich ausführen:

```
linux:~$ avkclient avkversion - gibt Version und Updatedatum der Virensignaturen aus  
linux:~$ avkclient version - gibt Version in Kurzform aus  
linux:~$ avkclient scan:<file> - scannt die Datei <file> und gibt das Ergebnis aus
```
- 4** Sehen Sie sich die Konfigurationsdatei an: Unter **etc/gdata/avclient.cfg** finden Sie die Konfigurationsdatei des Remoteclients **avclient**. Kontrollieren Sie, ob die Adresse des Haupt-Management-Servers (MainMMS) korrekt eingetragen ist. Falls nicht, löschen Sie den falschen Eintrag und melden den Linux-Client über den G Data Administrator erneut an oder tragen Sie die Adresse des G Data ManagementServers direkt ein.
- 5** Testen Sie Ihre Freigaben: Der Virenschutz für die Samba-Freigaben wird durch den Eintrag **vfs objects = gdvfs**

in der Samba-Konfigurationsdatei **/etc/samba/smb.conf** aktiviert. Steht der Eintrag in der Sektion **[global]**, so ist der Schutz für alle Freigaben aktiviert. Steht die Zeile in einer anderen Sektion, so gilt der Schutz nur für die entsprechende Freigabe. Sie können die Zeile testweise auskommentieren (eine Raute (#) voranstellen), um festzustellen, ob der Zugriff ohne den Virenschutz funktioniert. Falls nicht, suchen Sie zunächst den Fehler in Ihrer Samba-Konfiguration.

6 Linux Workstation Wächter

Prüfen Sie, ob der Wächter-Prozess **avguard** läuft:

linux:~# ps ax|grep avguard

Der Wächter benötigt die Kernel-Module **redirfs** und **avflt**. Sie können mit **lsmod** prüfen, ob die Module geladen sind: **lsmod|grep redirfs** und **lsmod|grep avflt**.

Die Module müssen für den von Ihnen verwendeten Kernel kompiliert sein. Dies erledigt das **Dynamic Kernel Module System (DKMS)**, welches zusammen mit den passenden Kernel-Header-Paketen Ihrer Distribution installiert sein muss. Wenn das der Fall ist, kompiliert und installiert DKMS die Module automatisch. Sie finden die **Logdatei** des Wächters unter **/var/log/gdata/avguard.log**.

12.2 Installation der Client-Software auf Linux-Rechnern

Das Produkt ermöglicht es, den **G Data Virenschutz** auf **Linux-Workstations** verschiedener Distributionen einzusetzen. Der **Linux-Client** kann dabei (ebenso wie die **Windows-Clients**) in die Infrastruktur des G Data ManagementServers eingebunden und zentral über die G Data Administrator-Software gesteuert und mit Signaturupdates versorgt werden. Analog zu den Windows-Clients wird auch bei Linux-Clients ein Dateisystemwächter mit einer grafischen Benutzeroberfläche eingerichtet, die sich in der Funktionalität an der Windows-Version orientiert. Für Linux-Rechner, die als **Fileserver** arbeiten und verschiedenen Clients Windows-Freigaben (über das **SMB-Protokoll**) zur Verfügung stellen, kann hierzu ein Modul installiert werden, das den Zugriff auf die Freigaben kontrolliert und bei jedem Zugriff einen Scan auf die Datei ausführt, so dass keine Malware vom Samba-Server auf die Windows-Clients (und umgekehrt) gelangen kann.

Für den **Workstation-Client** ist eine Kernel-Version größer gleich 2.6.25 erforderlich, dies ist z.B. bei Ubuntu 8.10, Debian 5.0, Suse Linux Enterprise Desktop 11 und anderen aktuellen Distributionen der Fall. Bei anderen Distributionen ist im Einzelfall eine Anpassung erforderlich. Der **Fileserver-Client** lässt sich auf allen gängigen Distributionen verwenden.

Um die Software auf dem Linux-Client zu installieren, gehen Sie folgendermaßen vor:

- 1 Remote-Installation der Client-Software über das Netzwerk**
Wählen Sie im Aufgabenbereich **Clients** im Menü **Client-Einstellungen** den Befehl **G Data Client für Linux installieren** aus. Nun erscheint ein Dialogfenster über das Sie den Client definieren können, auf den die Client-Software kopiert werden soll. Der Rechner muss dazu im Netzwerk bekannt sein.
- 2** Verwenden Sie die Auswahl **Computername**, wenn auf dem Client-Rechner ein **Samba-Dienst** installiert ist oder wenn der Rechner im **Nameserver** des Netzwerkes registriert ist. Sollte der Name des Rechners nicht bekannt sein, verwenden Sie die **IP-Adresse** des Rechners.
- 3** Geben Sie nun das **Root-Kennwort** des Rechners ein. Für eine Remote-Installation muss ein Root-Kennwort vergeben sein. Standardmäßig ist dies unter einigen Distributionen (z.B.) Ubuntu nicht der Fall.
- 4** Drücken Sie nun auf die **Installieren**-Schaltfläche. Im Bereich **Status** sehen Sie, ob die Installation erfolgreich war.

Manuelle Installation der Client-Software

Im Verzeichnis **\Setup\LinuxClient** auf der Programm-DVD finden Sie die folgende Dateien

- **installer.bin** = Installer für den Linux-Client

- **uninstaller.sh** = Uninstaller für den Linux-Client

Sie können diese Dateien auf den Client-Rechner kopieren und zur Installation der Client-Software die entsprechende Datei starten. Zusätzlich finden Sie hier noch eine Datei mit den **Virensignaturen**. Da die Software nach der Installation aber automatisch die neuesten Virensignaturen vom Server bezieht, ist die Installation dieser Datei fakultativ:

- **signatures.tar** = Archiv mit Virensignaturen

13 FAQ Fehlermeldungen

Geben Sie hier den Text ein.

13.1 Einige Clients melden "Die Virendatenbank ist beschädigt.". Was ist zu tun?

Um einen optimalen Virenschutz zu gewährleisten wird die Virendatenbank regelmäßig auf Ihre Unversehrtheit geprüft. Bei einem Fehler wird der Bericht **Die Virendatenbank ist beschädigt** eingefügt. Löschen Sie den Bericht und laden Sie das aktuelle Update der Virendatenbank von unserem Server. Führen Sie anschließend auf den betroffenen Clients eine Aktualisierung der Virendatenbank durch. Kontaktieren Sie unsere telefonische Hotline, wenn der Fehlerbericht erneut eingefügt wird.

13.2 Fehlermeldung "Sie benötigen mindestens Microsoft Exchange Server 2007 SP1"

Sollten Sie die unten stehende Fehlermeldung erhalten, sind die Mindestvoraussetzungen für die Installation der G Data MailSecurity nicht erfüllt. Für eine Installation wird mindestens Microsoft Exchange 2007 mit Servicepack 1 benötigt. Dieser muss VOR der G Data MailSecurity installiert werden. Siehe hierzu auch [Installation](#) und [Systemvoraussetzungen](#)

13.3 Einige Clients melden "Programmdateien wurden verändert oder sind beschädigt". Was ist zu tun?

Um einen optimalen Virenschutz zu gewährleisten, werden die Programmdateien regelmäßig auf Ihre Integrität geprüft. Bei einem Fehler wird der Bericht **Programmdateien wurden verändert oder sind beschädigt** eingefügt. Löschen Sie den Bericht und laden Sie das aktuelle Update der Programmdateien (G Data Client) von unserem Server. Führen Sie anschließend auf den betroffenen Clients eine Aktualisierung der Programmdateien durch. Kontaktieren Sie unsere telefonische Hotline, wenn der Fehlerbericht erneut eingefügt wird.

Index

A

Abholung 96
Absenderfilter 93
Administrator 23
Aktivität 94
Aktualisieren 27
Alarmmeldungen 31
Allgemeines 3
Anfragen 96
Anhänge filtern 92
AntiSpam 53
AntiVirus Business 98
AntiVirus Client Installationspaket erstellen 28
Anwendungskontrolle 63
Aufgabenbereiche 37
Aufträge 54
Ausgehend 98
Ausgehend (SMTP) 96
AVM Ken 108

B

Beenden 27
Begrenzung 100
Benutzerkonto 102
Benutzerverwaltung 26
Berichte 73
Blacklist 103
BootScan 13

C

Client 45,83
Client deinstallieren 41
Client installieren 40
Clientauswahlbereich 36
Clients 38

D

Dashboard 37
Deaktivierte Clients anzeigen 27
Die Clients sollen nicht über ihre Namen sondern über ihre IP-Adresse angesprochen werden 108

E

Eingehend 97
Eingehend (POP3) 96
Eingehend (SMTP) 95
Einige Clients melden "Die Virendatenbank ist beschädigt". Was ist zu tun? 113
Einige Clients melden "Programmdateien wurden verändert oder sind beschädigt". Was ist zu tun? 113
Einrichtungsassistent 24
Einstellungen 32,100,101
E-Mail 50
Emergency-AntiViren Service 10
Empfang 95,96

Empfängerfilter 93
Erweitert 100
Exchange-Server 2000 108
Externe Referenzen deaktivieren 92

F

Filter 90,97,102
Firewall 66,85

G

Gerätekontrolle 63
Größenbegrenzung 100
Gruppe bearbeiten 28

H

HTML-Skripte deaktivieren 91

I

Ich möchte den Administrator auf einem Client-Rechner installieren 106
Ich möchte die Clients mit Hilfe der CD-ROM mit der Client-Software ausstatten 106
Ich möchte die Installation der Clients zentral vom Server aus über den Administrator durchführen 105
Inhaltsfilter 93,104
Installation 15
Installation der Clients 19
Installation der Client-Software auf Linux-Rechnern 111
Installation des Administrators 17
Installation des ManagementServers 16
Installation des WebAdministrators 18
Internet Update 28,85
Internet-Einstellungen 102
Internetnutzungszeiten 65
IP-Filter 94

J

Job 57

K

Kennwort ändern 101

L

Lastbegrenzung 34
Lesebestätigung filtern 91
Linux-Fileserver Clients: Es wird keine Verbindung zum ManagementServer aufgebaut / Signaturen werden nicht aktualisiert 110
Logging 101
Löschen 28

M

MailSecurity, Exchange-Server 2000 und AVM Ken! 108
ManagementServer 22
Mein Postfach wurde in die Quarantäne geschoben 108
Menüleiste des Administrators 95

N

Nach der Installation des Clients laufen
einige Anwendungen erheblich
langsamer als vorher 107

Nachrichten 42

Neue Gruppe 27

Nicht zustellbare Nachrichten 100

O

Optionen 84,95

P

PolicyManager 62

PremiumHotline 10

Profi-Einstellungen 104

Programmaufbau des
WebAdministrators 86

Programmbereiche des
Administrators 88

Programmdateien 29,102

Protokoll anzeigen 25

Q

Quarantäne 84

R

Realtime Blacklists 103

Rechnername 100

Regelsätze 68

S

Scanparameter 98

Schlüsselwörter (Betreff) 103

Schlüsselwörter (Mailtext) 104

Schutz vor Relaying 95

Security-Symbol 83

Server verwalten 26

Spam filtern 94

Spam-Filter 102

Sprachenfilter 94

Statistik 78

Status 37,89

Subnet-Server-Synchronisation 27

Synchronisation 33

Systemnachrichten 100

Systemvoraussetzungen 10

U

Übersicht 39,66

Update 101

Update-Rollback Engine A / B 32

V

Virendatenbank 29

Virenfunde 95

Virenprüfung 83,97

Virensignaturen 102

Vor der Installation 12,87

W

Wächter 47

Wächter ausschalten 83

Warteschlange 99

Warteschlangen 94

Web/IM 52

WebAdministrator 86

Web-Inhaltskontrolle 65

Weiterleitung 95,96

Whitelist 103

Wie kann ich überprüfen, ob die
Clients eine Verbindung zum
ManagementServer haben? 108

Z

Zeitplanung Viren-Update 101

Zugangsdaten 101

Zugangsdaten und Einstellungen 30